# PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-232348
(43)Date of publication of application : 27.08.1999

(51)Int.Cl. G06F 17/60
G06F 19/00
G07F 19/00
G07F 7/10

(21)Application number : 10-322533
(22)Date of filing : 12.11.1998

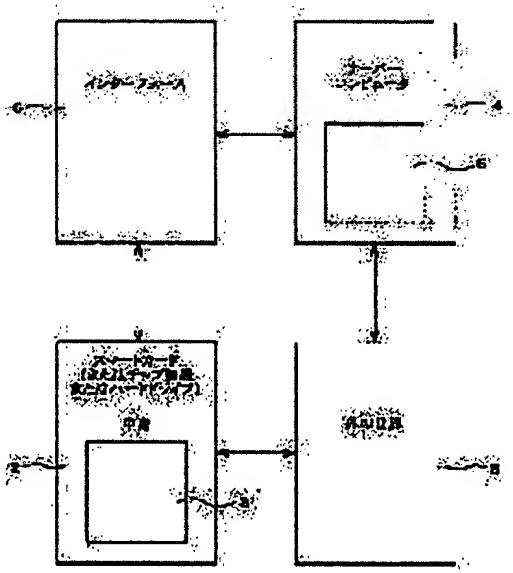
(71)Applicant : CITICORP DEV CENTER INC
(72)Inventor : PALTENGHE CRIS T
MAMDANI ALNOOR B
GOLVIN CHARLES
HENRY CHRISTIN
DAVID SOLO
JACK PAN
MELVIN M TAKATA

(30)Priority

Priority number : 97 65291 Priority date : 12.11.1997 Priority country : US
98 81748 14.04.1998
US

## (54) VIRTUAL WALLET SYSTEM

(57)Abstract:
PROBLEM TO BE SOLVED: To obtain a device for storing information and money by providing the device with an interface between a locally resident wallet part and a wallet part residing in an external server.
SOLUTION: A virtual wallet system is provided with a hybrid between a wallet 2 kept by an owner close at hand and a wallet arranged on a remote place together with a server 4 or the like. Namely the system includes the interface between the local function 2 and the server 4 and interacts with an external world 8 through the wallet 2 and/or the server 4. Thus the system is provided with the locally resident part and the part residing in the server 4 and these two wallet parts can be communicated with each other through the interface 6. Thus information including a payment mechanism, a personal identification mechanism, personal information, and an electronic artifact and money can be stored.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（A）**　(11)特許出願公開番号

**特開平11－232348**

(43)公開日　平成11年(1999)８月27日

| (51)Int.Cl.[6] | 識別記号 | ＦＩ | |
|---|---|---|---|
| Ｇ０６Ｆ　17/60 | | Ｇ０６Ｆ　15/21 | Ｚ |
| 19/00 | | Ｇ０７Ｆ　7/10 | |
| Ｇ０７Ｆ　19/00 | | Ｇ０６Ｆ　15/30 | Ｍ |
| 7/10 | | | Ｚ |
| | | | ３４０ |

審査請求　未請求　請求項の数13　ＯＬ　外国語出願　（全 59 頁）　最終頁に続く

(21)出願番号　特願平10－322533

(22)出願日　平成10年(1998)11月12日

(31)優先権主張番号　６０／０６５２９１

(32)優先日　1997年11月12日

(33)優先権主張国　米国（ＵＳ）

(31)優先権主張番号　６０／０８１７４８

(32)優先日　1998年４月14日

(33)優先権主張国　米国（ＵＳ）

(71)出願人　598156527
シティコープ　デヴェロップメント　センター，インコーポレイテッド
Ｃｉｔｉｃｏｒｐ　Ｄｅｖｅｌｏｐｍｅｎｔ　Ｃｅｎｔｅｒ，Ｉｎｃ．
アメリカ合衆国　カリフォルニア州　90066，ロスアンジェルス，ダヴリュー．ジェファーソン　ブールバード　12731

(72)発明者　クリス　ティ．パルテンゲ
アメリカ合衆国　カリフォルニア州　91326，ノースリッジ，エントレイド　アヴェニュー　11718

(74)代理人　弁理士　古谷　栄男　（外３名）

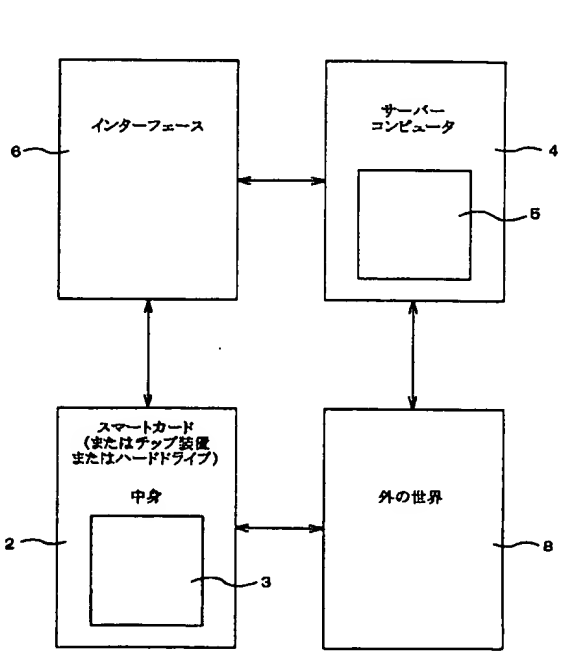
最終頁に続く

(54)【発明の名称】　仮想ウォレットシステム

(57)【要約】

【課題】　本発明は、情報および金銭保管用の装置、方法およびシステムを提供する。

【解決手段】　本発明の装置は、支払いメカニズムと、身元確認認証メカニズムと、個人情報と、電子アーチファクトとを含む、情報および金銭の保管を可能にする仮想ウォレットを含む。本発明の方法およびシステムは、仮想ウォレットを利用した情報および金銭保管方法を含む。好ましい仮想ウォレットは、ローカルに常駐している部分と、サーバーに常駐している部分とを備える。インタフェースを提供してウォレットのこれら２つの部分の間で通信できるようにする。



1

【特許請求の範囲】

【請求項１】ローカルに常駐しているウォレット部分と、外部のサーバーに常駐しているウォレット部分と、ローカルに常駐しているウォレット部分と外部のサーバーに常駐しているウォレット部分との間のインタフェースと、を備える仮想ウォレットシステム。

【請求項２】前記ウォレットが、支払いメカニズムと、身元確認認証メカニズムと、個人情報と、電子アーチファクトとのうちの少なくとも１つを備える請求項１に記載の仮想ウォレットシステム。

【請求項３】前記支払いメカニズムが、銀行口座情報と、クレジットアカウント情報と、電子通貨と、電子小切手と、キャッシュカードとのうちの１つまたは複数を備える請求項２に記載の仮想ウォレットシステム。

【請求項４】前記身元確認認証メカニズムが、個人識別情報と、認証情報とを備える請求項２に記載の仮想ウォレットシステム。

【請求項５】前記個人情報が、名前と、自宅住所と、職場住所と、自宅電話番号と、職場電話番号と、緊急連絡先情報と、個人的な電話番号および住所と、約束および覚え書きと、個人の好みおよび関心事と、バイオメトリック情報とのうちの１つまたは複数を備える請求項２に記載の仮想ウォレットシステム。

【請求項６】前記個人識別情報が、名前と、自宅住所と、職場住所と、自宅電話番号と、職場電話番号と、緊急連絡先情報と、バイオメトリック情報とを備える請求項５に記載の仮想ウォレットシステム。

【請求項７】前記認証情報が、証明書と、アクセスキーと、バイオメトリック情報とのうちの１つまたは複数を備える請求項５に記載の仮想ウォレットシステム。

【請求項８】前記電子アーチファクトが、ローヤルティクレジットと、クーポンと、写真と、トークンと、チケットとのうちの１つまたは複数を備える請求項２に記載の仮想ウォレットシステム。

【請求項９】請求項１に記載の仮想ウォレットを利用した電子取引用のシステム。

【請求項１０】前記インタフェースが、ローカルに常駐しているウォレット部分と外部のサーバーに常駐している部分との間のデータ転送を可能にする請求項１に記載の仮想ウォレットシステム。

【請求項１１】前記外部のサーバーに常駐している部分が、ローカルに常駐しているウォレット部分に収容されている情報のミラーを含む請求項１に記載の仮想ウォレットシステム。

【請求項１２】外部のサーバーに常駐している部分がアプリケーションを含み、ローカルに常駐しているウォレット部分が、外部のサーバーに常駐している部分に常駐するアプリケーションへの接続を備える請求項１に記載の仮想ウォレットシステム。

【請求項１３】前記接続が、前記アプリケーションに対

2

する応諾許可ユーザを識別するキーのためのプロキシを備える請求項１２に記載の仮想ウォレットシステム。

【発明の詳細な説明】

【０００１】

【関連出願へのクロスリファレンス】本願は、１９９７年１１月１２日に発明の名称"DISTRIBUTED NETWORK BASED ELECTRONIC WALLET"として出願された仮特許出願第６０／０６５，２９１と、１９９８年４月１４日に"VIRTUAL WALLET SYSTEM"として出願された仮特許出願第６０／０８１，７４８について、米国特許法第１１９条（ｅ）に従って優先権を主張するものである。上記各出願の開示は、これらを参照して、この出願に合体される。

【０００２】

【発明の分野】本発明は、情報および金銭保管用の装置、システムおよび方法に関する。本発明の個々の特徴としては、個人財務情報を含む個人情報の格納、検索および管理用の電子ウォレット(Wallet))およびコンピュータならびに関連した電子装置ベースのシステムが挙げられる。本発明の他の特徴は、デジタル署名用のシステムである。

【０００３】

【背景】インターネットおよび他の電子トランザクション媒体が爆発的人気となり普及するにつれて、電子フォーマットでの情報に対する需要および依存性は常に増大してきている。しかしながら、消費者の電子データ全てを格納、検索および管理する上での問題は、いまだに満足のいくレベルで分析または解決されていない。

【０００４】さらに、この問題は、現時点では消費者側の視点に立ったアプローチではなく、各業者の要求を満たすための業者側からみたアプローチである。上述した需要のうちいくつかを扱う製品の形態の１つが通常は電子ウォレットと呼ばれているものである。一般に、既存の電子ウォレットは、業者が使用して他の製品を機能強化するための後付的なものにすぎない。通常、電子ウォレットは、ネットワーク上またはブラウザ内のソフトウェアアプリケーションであり、さらに大きなプログラムの一部をなしている。電子ウォレットは主に電子取引での支払いという側面に焦点を当てている。例えば、電子ウォレットは、業者によって販売される主製品で実行可能な、権限のある電子トランザクションにおいて使用されるクレジットカードアカウント情報およびデジタル証明書を有している。

【０００５】また、電子ウォレットの操作は一般に全世界共通のものではない。１つの業者の電子ウォレットアプリケーションに追加された情報は、他のアプリケーションで使用したり他のアプリケーションからアクセスしたりできない場合がある。事実、プログラムを提供している業者は、そのプログラムに関連した電子ウォレットアプリケーションを１つだけしか使用しないようにと要

求する場合がある。このため、消費者は自分の電子ウォレットの構成要素を構築するのに必要なデータおよび情報を繰り返し入力して獲得するといった、フラストレーションを生じるタスクを強いられることになる。

【０００６】さらに、既存の電子ウォレットは主に、それよりもさらに大きなアプリケーションの一部として設計されているため、一般に機能面では制限がある。既存の電子ウォレットは通常、クレジットカードアカウント情報またはデジタル証明書などの特定の予め指定された種類の電子情報を保持できるのみである。一般に、既存の電子ウォレットを利用しているアプリケーションは支払い機能のみを必要とすることがあり、よって電子ウォレットはこの機能しか提供しない。通常、既存の電子ウォレットの機能性は、消費者ではなく業者の需要に応じて動かされる。一方、電子ウォレットと自分の生活に関わるあらゆる面とを一体化することを求めている消費者は、複数のデータソースからの様々なデータを格納、管理、検索する機能を必要としている。このため、個々のソフトウェア業者側の需要ではなく電子ウォレットの所有者側での需要に基づいて選択される電子データでも機能できる電子ウォレットに対する需要がある。

【０００７】また、電子ウォレットは一般に、スマートカード内またはパーソナルコンピュータ上など所有者の手元に置いてあるか、あるいはサーバー上など所有者から離れた所に置いてある。どちらに置いておく場合にも欠点がある。

【０００８】手元に置いておくと、所有者が完全に制御でき仮想ウォレット発行者によって多くのリソース割り当てを要求されることがないという利点がある。一方、電子ウォレットを手元に置いておくことで、例えばスマートカードの紛失または盗難、あるいはパーソナルコンピュータのハードドライブのクラッシュなど所有者側での紛失の危険も高くなる。さらに、パーソナルコンピュータに置いてある場合には、セキュリティ、携帯性および操作の共通性の問題が起こる。ネットワーク接続されたコンピュータがハッキングされ、このため自分の価値ある情報を暴露してしまうこともある。また、多くの家庭用コンピュータは移動式ではないため、所有者が電子ウォレットを使うことのできる範囲は限られてしまう。最後に、手元のブラウザなどのプログラム中に置いておくと、通常は所有者が競合するブラウザを便利に利用しにくくなるよう制限がかかり、他のアプリケーションとの互換性が制約される。このように、手元に置くことには幾つかの欠点がある。

【０００９】遠隔地にある電子ウォレットは一般にサーバー上に置かれている。サーバーが紛失したり盗難にあったりすることはないため、この選択肢をとれば情報に対する保護性は高くなるという利点がある。しかしながら、サーバーに置いておくと所有者がウォレットにアクセスするためには何らかのネットワーク接続を構築する必要がある。さらに、遠隔地から情報にアクセスすることで、アクセス要求を出している個人の身元確認の認証面で問題が生じる。パスワードおよび個人身元確認番号（PIN）を使用して情報に対する保護性を高めることもできるにはできるが。このように、遠隔地に置くことには幾つかの欠点がある。



【００１０】したがって、既存の電子ウォレットにおける上述した欠点のいくつかまたは全てを克服し、情報保管用の新たな装置、方法およびシステムを提供する必要性がある。

【００１１】

【発明の概要】本発明によれば、情報および金銭保管用の装置、方法およびシステムが得られる。本発明の装置は、情報および金銭保管を可能にする仮想ウォレットを含む。本発明の方法およびシステムは、仮想ウォレットを用いた情報および金銭保管方法を含む。

【００１２】本願明細書において、金銭保管は、従来から金融サービス産業において行われてきた保管、投資およびセキュリティサービスを意味する。情報保管または情報ベースの保管は、顧客のために大切な情報を安全な場所に格納する財務的隠喩(financial metapher)を拡張したものである。本発明では、情報は貨幣と似たような方法で取り扱われる。だが、「情報および価値」は「データおよび貨幣」としての方が互いに似通っている。金庫保管される情報の例としては、財務および信用履歴の他に、保険証券、法的文書、医療記録などを挙げることができる。

【００１３】本発明のもとでは、「貨幣」の格納および価値評価を特徴とする理論的な装置および実用的な装置の両方を通して消費者の個人情報を見ることができる。例えば、金庫を用いて貨幣を格納することは、情報を格納および保護することの隠喩として用いることができ、貨幣の投資はその情報をトランザクションに利用して価値を生み出すことの隠喩として用いることができる。このように、本発明は、情報を金庫保管および投資するための装置、システムおよび方法を個人に提供するものである。

【００１４】本発明の一実施形態は仮想ウォレットである。仮想ウォレットは、物理的な隠喩すなわち従来のウォレットの電子版としての概念であることができる。一側面において、本発明の仮想ウォレットは、コンテナとして機能する特別なハードウェアに含ませることが可能な、支払いメカニズム、身元確認認証メカニズム、個人情報および電子アーチファクトのうちの少なくとも１つのための、仮想ウォレットの所有者／ユーザ用ソフトウェアを有する。また、本発明の仮想ウォレットは、個人情報を安全に格納、検索および管理するための電子システムを有するものとしての概念であることもできる。

【００１５】上述したように、本発明の仮想ウォレットは、ウォレットの所有者／ユーザの支払いメカニズム、

5

身元確認認証メカニズム、個人情報、電子アーチファクトなどを含むがこれに限定されるものではない電子オブジェクト用のコンテナとして機能する。これらの電子オブジェクトは、好ましくは、例えば金融サービス施設などの単一のソースからの情報に限定されるものではない。むしろ、本発明の仮想ウォレットを利用して、複数の金融機関を含む様々なソースからの情報および様々なソースからの個人情報を保持し、ユーザに一層有用な仮想ウォレットを提供することができる。従来のウォレットのユーザの多くは、様々なソースからの複数の銀行カード、クレジットカード、個人情報、メモ書き、メンバーカードなどを持つのに自分のウォレットを使用している。この点に関しては、本発明の仮想ウォレットは、好ましくは従来のウォレットと同様の各ウォレットに含まれる情報の種類およびタイプの面で従来のウォレットと類似している。

【００１６】本発明によれば、仮想ウォレットは以下の特徴のうち１つまたは複数を有していてもよい。本発明の仮想ウォレットでは、所有者がその中身をパーソナライズして、所有者が望むどのような情報であっても所有者が選択したフォーマットで格納できるようにすることができる。また、仮想ウォレットの所有者はどこにいてもウォレットの中身にアクセスすることができ、パーソナライズしたフォーマットであることに加えてウォレットは最大限に便利なものとなる。さらに、本発明の仮想ウォレットでは、所有者がウォレットに格納された情報と他の機能とを結びつけることができる。これによって、格納されている情報の実用性が影響を受け、仮想ウォレットを他のアプリケーションと共通操作できるようになる。さらに、本発明の仮想ウォレットでは、所有者はウォレット内の情報へのアクセスおよびその配信を制御して、所有者に彼／彼女の個人情報に対するセキュリティおよび完全な制御を持たせることができる。本発明の仮想ウォレットシステムは、仮想ウォレットの所有者が自分の情報を配信できるという利点を提案するという有利な特徴を有するものである。本発明の仮想ウォレットのさらに他の特徴は、ウォレットの中身を遠隔地にて格納および／または使用禁止にすることで、ウォレット内の情報を紛失する危険をなくす１つまたは複数のメカニズムとなってもよいことである。このように、本発明の仮想ウォレットは、情報および価値ある金融アイテムを保持するための信頼できる場所になり得ると同時に、情報を移動させる上での便利な方法にもなり得るという有利なものである。

【００１７】仮想ウォレットに格納される支払いメカニズムは、例えば銀行口座情報、掛け売り勘定情報、電子通貨、電子小切手およびキャッシュカードなどを有していてもよい。仮想ウォレットに格納される身元確認認証メカニズムは、個人識別情報および認証情報を含んでもよい。個人身元確認情報は、例えば、名前、自宅住所、

6

職場住所、自宅電話番号、職場電話番号、緊急連絡先情報およびバイオメトリック情報を有していてもよい。認証情報は、証明書などの物体、アクセスキーおよびバイオメトリック情報を有していてもよい。仮想ウォレットに格納される、所有者の個人情報およびアーチファクトは、例えば、上述したような個人身元確認情報、その他の個人的な電話番号および住所、約束および覚え書き、個人の好みおよび関心事、ローヤルティクレジット、クーポン、写真、トークンおよびチケットなどを有していてもよい。上述したオブジェクトは仮想ウォレットの徹底した機能のうちのいくつかの一例にすぎない。本願明細書を読み終われば当業者には他の例も明白になろう。

【００１８】本発明の仮想ウォレットの利点の１つは、仮想ウォレットに様々なソースからの情報を含み得るということである。さらに、異なるソースからの情報が相互作用することもある。例えば、マイレージサービス付きクレジットカードを含む本発明の仮想ウォレットでは、ウォレットの所有者はクレジットカード情報およびマイレージポイントを管理およびトラッキングする付加価値機能の両方を管理およびトラッキングすることができる。また、本発明の仮想ウォレットなどの電子ウォレットでは、消費者がウォレットの発行者とは関係のないアイテムを追加することもできる。ウォレットにどのようなアイテムでも追加できるようにすることで、消費者および他のアプリケーション業者にとっても利点がある。

【００１９】本発明の仮想ウォレットのもう１つの利点は、仮想ウォレットが有利に、情報および価値ある金融アイテムを保持する信頼できる場所になり得るということである。現在、電子トランザクションのプライバシーおよび安全性に関する、分かっているものおよび分かっていないものを含む消費者の心配事は多くある。選択肢を与えられれば、消費者が怪しい第三者ではなくすでに信頼および消費者支持面で定評のある者に自分の重要情報を預けることは論理的である。消費者についての情報が秘密で集められ、市場に流れて販売されていくことが次第に増えている世界では、プライバシー保護および安全性の明白なポリシーは、金融機関からの仮想ウォレットを保持する強力な動機である。さらに、消費者情報を持つ際に価値があるだけでなく、これを移動する際にも価値がある。貨幣と同様に、情報を投資してリターンを増やすこともできる。また、情報は保護されなければならず、これによって情報金庫および安全な預金ボックスの概念が生まれる。プライバシーに関する中心的な問題は機会に変わり、情報保管の中心にある。

【００２０】本発明の仮想ウォレットのさらに他の利点は、仮想ウォレットによって情報を移動させる便利な方法が得られるということである。本願と同日に出願され、出願番号＿＿＿＿＿＿を付与された、本願発明者らの発明の名称"DISTRIBUTED NETWORK BASED ELECTRONI

C WALLET"（情報保管用の方法およびシステム）である係属中出願（その内容全体を本願明細書に引用する）においてさらに詳細に説明してあるように、非常に便利であるシンプルなサービスは、消費者が情報バンクに置いてある自分の個人データからウォレットを介してフォームを埋めるのを助けることである。ローン申請、敷地の登記、仕事の申請などは、一度情報を知られたら、次の時に別の理由であったりあるいは別のオーダーの時であったとしても、消費者がこれを再度タイピングしなければならない理由はない。さらに他の特徴は、その時に示したい相手（例えば社会対仕事など）に応じて、仮想ウォレットの所有者が同じ質問に対して何度も答えることができることもあるという点である。

【００２１】本発明の仮想ウォレットのさらに他の利点は、仮想ウォレットが選択的な紛失、盗難および災害からの回復可能性を提供するという点である。現在のウォレット設計の多くは、ウォレットを紛失したり、あるいは盗難または災害によって破壊されたりした場合に不備がある。これらの不幸な災難のうちいずれかが起こった場合に、自分の人生が破滅していないことが分かれば、消費者にとって利点がある。本発明のシステムの一実施態様では、データの損失または破壊なしに新たな仮想ウォレットを発行することができる。ウォレットが盗まれた場合でも、泥棒がその情報を利用できる可能性は低く、消費者のアカウント状態またはウォレット内のアイテムに影響することなくウォレットのキーを遠隔地から使用禁止にすることができる。

【００２２】本発明の仮想ウォレットのさらにもう１つの利点は、仮想ウォレットによって遊牧民的（ノマディック(nomadic)）なアクセスが可能になるという点である。現在のウォレット設計では、自分のウォレットのアイテム（特に証明書）を受け取る時に機械が制限されるだけでなく、それを得た特定のブラウザにも制限がある。このため、消費者が自宅でＳＥＴ証明書を入手してこれを職場で使いたい場合など彼らにとっては極めて不便である。本発明は、ノマディックな解決策を提供し、消費者がどこにいてもウォレットを使用できるようにする。

【００２３】本発明の仮想ウォレットのさらに他の利点は、仮想ウォレットを買い物の補助的なものにすることができるという点である。消費者情報を持っていることで、結果として彼らが何に興味を持っているのかを推定する機能が得られる。本発明の仮想ウォレットシステムによって、ウォレットの発行者は、消費者が自分の買いたいものを見つけるのを助ける、信頼できる電子仲介業者になる機会を得ることができる。さらに、消費者が何に興味を持っていないのかを知ることで、彼らの電子従者になって不用なスパム(spam)を分別除去する機能が得られるという結果もある。支払いが取引のほんの一部でしかないということを認識し、取引の他の部分に注目することで、本発明の仮想ウォレットによって消費者およびウォレットの発行者の両方にさらなる利点がもたらされる。



【００２４】本発明の仮想ウォレットのさらに他の利点は、仮想ウォレットが情報オーガナイザーでもあり得るという点である。この点に関しては、本発明の仮想ウォレットは個人情報を管理および編成するための有用かつ便利な方法を提供する。さらに、本発明の仮想ウォレットの個人情報システムは、有利に、保護された情報バンクの一部を形成することができる。

【００２５】本発明の仮想ウォレットのさらにもう１つの利点は、仮想ウォレットが金融および非金融利得を生成できるということである。本発明の一実施態様において、ウォレットパッケージの一部が考えられる複数のストラテジーに基づいた利得の特徴となり得る。第１のストラテジーでは、ウォレットの持ち主が利用できる割引および特別売り出しを行う。これは、金融サービスプロバイダにとっては馴染みのある技術であり、今日カードおよびメンバーシッププログラムですでになされているものから極端に外れるものではない。しかしながら、一般に、割引および売り出しは一斉送信的な側面を持つものであり、必ずしも特定消費者の本当の興味に一致するとは限らない。このため、割引および売り出し情報を配布するためのコストの中には、興味のない消費者のために浪費されているものもある。

【００２６】本発明の仮想ウォレットシステムによって可能になった、上記のものよりも広いストラテジーでは、消費者を鼓舞し、自分の情報アカウント（ウォレットの中身）と金融アカウントとをペアにして利用できる実態的人口統計（demographics）および興味のあるものを作成させる。まず最初に、消費者は自分たちが関心のあるものを特定するよう指示され、電子ショッピング代理店は彼らに自分たちが見つけたものを報告する。次に、消費者が興味を持っているものを、彼らの身元ではなくプロファイルごとに分類し、データベースに入力する。消費者からはマイナスの面が認められている、プロファイル化後の名簿を販売する代わりに、マーケティング担当者は特定のプロファイルの仮想ウォレットユーザに配布される電子広告を持つために代金を支払う。

【００２７】ウォレットの背後にある情報バンクは、消費者の身元確認情報を保管しつつ、マーケティング担当者が利用できる価値ある情報を作成している。この種のマーケティングレスポンスはプライバシー侵害だと考えられることは少ない。消費者は何らかのアイテムを探す検索を行って自分が興味を持っているものを示したからである。

【００２８】ウォレットの価値の問題は、配布に対する対価としてマーケティング担当者から受け取る金銭の一部が消費者の金融アカウントを介して彼らに渡るということである。要するに、マーケティング担当者は消費者

に対して、彼らからの提案を検討するのに消費者が割いた時間に対する対価を支払うことになる。マーケティングメッセージは消費者個人のプロファイルを通してスクリーニングされるため、消費者は自分が述べた興味内容から大きく外れるものを何ら受け取ることはない。マーケティング担当者は、広告を配布するための投資をする前に、要求されたプロファイルに一致する個人が何人いるかのカウントを集計し、価格の見積を立てることができる。これによって、マーケティング担当者は、現金の大きな経費をかける前に自分のプロファイルの定義を洗練し、自分たちのマーケティングメッセージを手直しすることができる。これは、明らかに消費者およびマーケティング担当者の双方にとって満足のいくシナリオである。ウォレットのインタフェース隠喩を利用して消費者が自分たちの見返り対価をトラッキングするのを助けることができ、彼らが自分の情報を「金庫」エリアからプロファイルサーチャーが情報を利用できる「情報投資」エリアに出し入れして移動できるようにすることができる。

【００２９】この概念の変形例は、ローヤルティクレジットなどの非貨幣利得を有する消費者に報いるものである。ローヤルティクレジットは、キャッシュでの等価なものよりも高いとみなされている価値を合法的に持っている。現在、需要の高いローヤルティプログラム（例えば、マイレージポイントなど）は一般に大企業に限られ、利得は極めて流動性のあるものではない。マーケティングメッセージを見る代わりにローヤルティクレジットを受け取ることに加え、仮想ウォレットプロバイダは仲介手数料および他の人と様々なローヤルティクレジットを「交易」する交換サービスも提案することができる。これは、交換哲学の速度を増すことと一致し、ローヤルティプログラムの集合体に全体として利益のあるインパクトを与える。自分たちの債務を早期に救済することができるため、供給者側にも利益がある。いずれにしても消費者は、自分たちが頻繁に購入しようと考える製品に対するローヤルティプログラムに加入するので「ローヤルティ」の目的は依然として満たされる。消費者がクレジットの対価として交換できるものの幅が広がり、有効期限が来て稼いだクレジットが失われる潜在的な可能性が少なくなるため、消費者にとって全体としての価値は高くなっていく。消費者およびマーケティング担当者の双方にとって明らかに満足のいくもう１つのものは、同じメカニズムを介してなされる。本発明に関するさらに詳細な内容は、添付の図面および以下の説明に示してある。

【００３０】

〔発明の詳細な説明〕本発明によれば、個人が自分の金融情報および個人情報を管理できるようにする装置、システムおよび方法が得られる。本発明の実施態様を本願明細書では仮想ウォレットと呼ぶ。本発明は、仮想ウォレットと、仮想ウォレットシステムと、仮想ウォレットを利用するための方法とを含む。



【００３１】本発明の実施態様および特徴について、添付の図面を参照して詳細に説明する。

【００３２】図１は、本発明の考えられる実施態様を示す。本発明による図１を参照すると、仮想ウォレットは、所有者の手元２に置いてあるウォレットと、サーバー４と一緒にあるなど遠隔地に置いてあるウォレットとのハイブリッドを備えていてもよい。仮想ウォレットシステムはさらに、ローカルな機能２とサーバー４との間のインタフェース６を含む。仮想ウォレットシステムは、ローカルなウォレット２および／またはサーバー４を介して外の世界８と相互作用してもよい。ハイブリッド仮想ウォレットは、ローカルなウォレットの携帯性、所有者の制御および発行者のリソースが最小限ですむことと、遠隔地のウォレットのセキュリティおよび格納機能とを兼ね備えたものである。このように、ハイブリッド仮想ウォレットはそれぞれの置き場所の利点を有利に最適化する。以下の説明では、ウォレットのローカルな置き場所またはウォレットの一部を、これらの名前で呼ぶかまたは「クライアント」とする。ウォレットの遠隔地にある置き場所については、その名前で呼ぶかまたは「サーバー」とする。

【００３３】ウォレットのローカルな置き場所は、例えば、所有者のパーソナルコンピュータ、スマートカード、またはウォレットをオフラインで利用できるようにする同様の装置を含んでもよい。一般に、仮想ウォレットのローカルな態様すなわちローカルな内容３は、ウォレットの所有者が重要であると判断したデータおよび情報を含み、ウォレット全体は遠隔地に収容されている。例えば、仮想ウォレットのローカルな態様は、格納された値のがま口、重要な個人情報および認証情報、仮想ウォレットのローカルな態様がウォレット全体に含まれる機能のいずれをもエミュレートできるようにするアカウント情報を含んでもよい。所有者は、有利に、遠隔地から利用可能な便利なパッケージでウォレットの最も重要な態様を定義してこれにアクセスすることができる。好ましくは、ウォレットのローカルな態様を遠隔地のウォレットまたはサーバーにミラーで持ち、カードを交換しなければならないなどの場合に情報を保護する。さらに、ウォレットのローカルな態様は、所有者が遠隔地からサーバー上の仮想ウォレット全体にアクセスできるようにするための証明書または他の同様の認証指示を含んでもよい。このように、所有者はウォレットのローカルな態様をサーバーに接続することのできる様々な場所でウォレットの機能全てに対してアクセスすることができる。

【００３４】仮想ウォレットの遠隔地の態様は、有利に、ウォレット内の全ての情報に対するセキュリティを提供する。また、サーバーは、例えばスマートカードや

パーソナルコンピュータなどに比べると大きな情報の格納容量を提供する。仮想ウォレットの遠隔地の態様の中身５は、ウォレット全体を含み、その一部は仮想ウォレットのローカルな態様にミラーリングしてあってもよい。しかしながら、仮想ウォレットの遠隔地の態様は、オフラインでのトランザクションがゆえに、ウォレットのローカルな態様における完全なミラーキャッシュまたはキャッシュのようなオブジェクトではない。しかしながら、本発明は、ローカルなウォレットがオンラインにあるときに仮想ウォレットのローカルな態様から得られる最新の情報で仮想ウォレットの遠隔地の態様を更新する。また、本発明の有利な特徴によれば、仮想ウォレットの遠隔地の態様によって例えば所有者の身元および住所などをウォレットのサーバーだけしか知らない秘密情報に交換することで、トランザクションにおけるプライバシーを保護することができる。例えば様々な所有者の習慣、好みなどに関する情報にマーケティング担当者が代金を払い、所有者の身元を傷付けることなく情報を与える場合などにこの特徴を利用することができる。このように、仮想ウォレットの遠隔地の態様によって、セキュリティおよび格納機能が得られる。

【００３５】このように、本発明の仮想ウォレットの本実施態様は、ローカルな置き場および遠隔地の置き場の最も利点の大きな態様を相乗効果的に組み合わせて１つの仮想ウォレットとしている。ウォレットのローカルな態様は便利なオフライントランザクション用として使用され、一方、ウォレットの遠隔地の態様では紛失および盗難に対して保護できる。

【００３６】図２は、本発明のハイブリッド仮想ウォレットの実施形態およびこれを使用するための方法を概略的に示したものである。図２に示されるように、仮想ウォレットシステムは、パーソナル格納装置１２と、団体のサーバー１４と、インタフェース装置１６とを備えることができる。パーソナル格納装置１２および団体のサーバー１４は、各々外の世界１８と相互作用できる。

【００３７】パーソナル格納装置は、スマートカード、パーソナルデジタルアシスタント（ＰＤＡ）またはメモリチップ装置を備えていてもよい。パーソナル格納装置はまた、コンピュータのハードドライブまたは他のコンピュータベースの記憶装置を備えていてもよい。パーソナル格納装置の好ましい実施形態は、手持ち式で容易に移動可能なものであろうと、あるいはコンピュータのハードドライブの一部であろうと、ウォレットの使用者の好みに左右される。

【００３８】パーソナル格納装置は、以下のタイプのデータすなわち、プライベートキー、アカウント番号、電子通貨（ｅ－通貨）、クーポン、トークン、チケット、ローヤルティクレジットなどのうち１つまたは複数を含んでもよいが、これに限定されるものではない。パーソナル格納装置の機能は、以下のものすなわち、認証、デジタル署名または支払いのうち１つまたは複数を含んでもよい。これらのデータタイプおよび機能については、以下のセクションにおいてより詳細に説明する。ウォレットがスマートカード上にある場合には、消費者は本当の意味で「ノマディック」になり、どこに行っても自分のカードを差し込んで自分のウォレット（およびブックマーク）を常時利用することができる。しかしながら、クライアントに（および場合によってはサーバーにも）このローミング機能を可能にできるような仕組みを構築する必要が生じる。消費者にとってのカードの重要性が増せば増すほど、クレジットカード、免許証および他の物理的なＩＤカードでの交換プロセスの場合のような、紛失または盗難に遭ったカードを交換するための手段を開発しておかなければならない。これは、本当に有用な信頼できるウォレットプロバイダによって提案されるサービスの一部である。

【００３９】インタフェース装置はデータを含む必要はないが、通常は以下の機能すなわち、ユーザインタフェース相互作用、通信、または公開暗号化のうち少なくとも１つを含む。上述した説明から理解できるように、パーソナル格納装置がコンピュータのハードディスクをなし、インタフェース装置が同一のコンピュータをなしている場合、インタフェース装置はパーソナル格納装置のデータおよび機能を含んでいてもよい。

【００４０】団体のサーバーは、パーソナル格納装置と同一のデータを含んでもよく、さらに以下のタイプのデータすなわち、証明書、名前、住所、ログ履歴などのうち１つまたは複数を含んでもよい。団体のサーバーは、好ましくはパーソナル格納装置用のバックアップ手段として機能し、よってパーソナル格納装置に収容されているデータのバックアップコピーを含んでいるとよい。団体のサーバーは、以下の機能すなわち、認証、デジタル署名、支払い、ログ記録、報告および通信のうち１つまたは複数を含んでいてもよい。これらの機能および上述したデータタイプについては、以下のセクションにおいてさらに詳細に説明する。

【００４１】図２において大きな矢印で示されるように、パーソナル格納装置１２と、インタフェース装置１６と、団体のサーバー１４とは、セキュア・インタフェース・インタラクション１３を介して通信可能である。この点に関しては、インタフェース装置は、パーソナル格納装置１２と団体のサーバー１４との間のインタフェースを提供する。パーソナル格納装置１２は、ポイント・オブ・セールス・トランザクション１５の目的で外の世界１８と通信することができる。これらのトランザクションは、通貨の移動を必要とするトランザクション（例えば買い物）を含み、個人情報の移動を必要とするトランザクションも含む。仮想ウォレットの団体のサーバー部分１４は、仲介されたインターネット・トランザクション１７を介して外の世界１８と通信することがで

きる。これらのトランザクションは、現在のインターネットベースのトランザクションでのものと同様に取扱うことができ、金融情報（金銭保管）または個人情報（情報保管）の両方に関与する。

【００４２】テクノロジーの視点から、仮想ウォレットは、スマートカード、クライアントＰＣ／ＰＤＡ／ＳＴＢおよび／またはサーバー上に置かれるソフトウェアプログラムを含む。これらのプログラムは、少なくとも以下の４つのコンポーネントを実現する。

【００４３】ユーザインタフェース（ＵＩ）。ウォレットとその消費者との間の相互作用は、ユーザインタフェースコンポーネントによって制御される。

【００４４】挙動。挙動は、「支払い」「支払いタイプ追加」「個人情報編集」のようなものである。これらはウォレットの所有者がＵＩを介して利用できる挙動である。

【００４５】プロトコル。プロトコルは、ＳＥＴ、ＶＩＳＡキャッシュ、Ｍｏｎｄｅｘ、ＯＰＳを含む（下記参照）。これらは、ウォレットがどのようにして他のシステムおよびサーバーと相互作用する必要があるかについての定義となる。様々なシステム・インプリメントがこれらのプロトコルを実現するモジュールを提供する。

【００４６】中身（コンテンツ）。中身は消費者の具体的な支払いアカウント（クレジットカード、キャッシュカード、現金）および情報である。このデータは消費者毎に一意である。

【００４７】図３は、本発明の仮想ウォレットシステム２７１についての考え得るアーキテクチャを示す。上述したように、電子ウォレットの概念は多くの人々にとって多くの物を意味する。今日の消費者が携帯している、お金や鍵、身分証明書、クレジットカード、チケットの他、時計や新聞、電卓、携帯式電話、ポケットベルなど消費者に移動情報および通信手段を提供するものなどの重要なものの代わりに用いられる、スナップ写真大のカラー画面のあるポケットサイズのコンピュータが挙げられる。この実施形態では、ウォレット２７１はポケットに入れて持ち運びされる物理的なものである。これは電子的な性質のものであるため、従来のウォレットでは実現できないような機能を付加することもできる。しかしながら、この種の装置のことを気にする消費者がゆえに、装置は非実用的なものとなっている。電子装置の中身をバックアップすることは技術的には可能であるが、現実には、消費者は少なくともこのような装置に対しては、現在自分のデータが入っている装置に対するのと同程度に無責任である。さらに、このようなウォレットがウォレットの提供者または他者との間に介入すれば、消費者に関する情報を他者が利用して利益を得て、消費者当人にはそのことを知らせない可能性があるなど、安全面で気に掛かることもある。このように、物理的なウォレットの延長、特に第三者のソフトウェアまたはハードウェア業者によって提案されたものが急に広く取り入れられるようになることは考えにくい。



【００４８】これとは対極をなすものとして、完全に仮想的なウォレットがある。これは物理的な装置ではなく、どこかにあるサーバー上の一組のアプリケーションである。この方法の主な欠点は、すべてのトランザクションを「オンラインで」すなわちサーバーに接続して行わなければならないという点である。これは費用がかさむ、および／または使いにくいという結果になりかねない。もう１つの問題はセキュリティである。

【００４９】本発明のシステムによって好ましいハイブリッドな方法は、データおよびアプリケーションのいくつかを物理的な装置上に置き、残りをサーバーに置くというものである。スマートカードは理想的にこの種のアプリケーションに適している。セキュリティおよびアクセス機能をカードに持たせ、大量のデータおよびアプリケーションをサーバーに持たせる形を基本としているためである。さらに、少量の電子キャッシュ・トランザクションなどオンラインで行うには費用がかかりすぎるトランザクションも、このようなスマートカード上に持たせると道理にかなう。このように、図３に示されるように、一実施形態における電子ウォレット２７１は、電子キャッシュ・アプリケーション・コンテナ２７３と、電子キャッシュ・アプリケーション・マネジャー２７５と、ユーザまたは認証モジュール２７７と、アプリケーション・マネジャーへの鍵２８１と、キー・リング・アプリケーション・コンテナ２８３と、外部アプリケーション相互運用性ＡＰＩ（アプリケーション・プログラム・インタフェース）２７９と、ユーザ・アプリケーション・オーガナイザおよびマネジャー２８５とで構成される。

【００５０】電子キャッシュ・アプリケーション・コンテナ２７３は、その名前から想像できるように、ｅ－キャッシュアプリケーション用の記憶装置である。重要な集合体を得るために、２種類以上のｅ－キャッシュをサポートしている。コンテナ２７３における記憶装置は、構成要素が各々ｅ－キャッシュの何らかの形として存する記録についてのみ十分に汎用的なものであり、コンテナ２７３内の実際の「オブジェクト」は実際のｅ－キャッシュアプリケーションへの「コネクタ」である。プログラミングすることで、ｅ－キャッシュアプリケーションをロケーションして開始することができる。ｅ－キャッシュマネジャー２７５は、ｅ－キャッシュ・アプリケーションをどのように追加して使用するかを汎用的な方法で示すソフトウェアである。ユーザ認証モジュール２７７を交換し、セキュリティおよび認証技術の発展に対応できるようにすることも可能である。スマートカードの実現前は、これを口座番号および個人の身元確認番号を尋ねるソフトウェアとすることができたが、現在の技術では、今日実現されている認証技術を用いて同じこと

15

をカードとサーバーとで実現することができる。将来を見込んで、他のセキュリティおよび認証技術がバイオメトリックスなどを使用してもよい。

【００５１】アプリケーション・マネジャーへの鍵２８１は、クレジット、借方、ｅ－小切手、身分証明、施設へのアクセスおよびその他のアプリケーションなどのキャッシュ以外のアプリケーションを管理するよう機能する。これはキー・リング・アプリケーション・コンテナ２８３の中身を維持するソフトウェアである。キー・リング・コンテナ２８３は、サーバー・アプリケーションへのコネクタを保持する。このコンテナは、上述したアプリケーション・マネジャーへの鍵２８１によって管理および維持される。スマートカードがさらに一般的に利用できるようになってからであっても、実際にアプリケーションを保持できるほど十分な大きさのものにはならないと思われる。代わりに、サーバーに置かれているアプリケーションへの「コネクタ」を保持する。「コネクタ」の最も重要な態様は、アプリケーションに対する権限のあるユーザの身元確認を助ける鍵または証明書である。結果、「キーリング」は鍵のコンテナになる。しかしながら、図４においてさらに説明するように、これは「本物の」鍵とは違う。

【００５２】具体的には、図４はウォレットおよびアプリケーション・アクセス・スキーム３０１を示す。この図において、アクセス装置の提供者、ウォレットの発行者およびアプリケーションの提供者の概念は、いずれも別々である。図４に示されるように、消費者はアクセス装置３０３を使用して自分の情報３０５にアクセスすることができる。アクセス装置３０３は、ＰＯＳあるいは誰かとの連絡場所になる箇所に設けられている。次に、ウォレットは、アクセス装置３０３と、ネットワークに対するアクセス装置サーバー３０７の接続部分とを使用して、ウォレット発行者のサーバー３０９と連絡を取る。次に、消費者は自分の説明によって適当なアプリケーションを識別する。この説明は、アプリケーションの提供者のサーバー３１３に送られるアプリケーション・キー・プロキシ３１１と関連している。

【００５３】上述したスキーム３０１において、消費者は、ＰＯＳまたは誰かとの連絡場所になる箇所に設けられている装置３０３を介して自分の情報にアクセスすることができる。この誰かは装置３０３以外のいくつかの存在を欲しがるため、「不動産」のいくつかは、その中身に関する呈示インタフェースからは外される。ウォレット２７１は、装置３０３および装置サーバー３０７のネットワーク３０１への接続部分を利用してウォレット発行者のサーバー３０９と連絡を取る。消費者は、上述したように、自分の説明によって適当なアプリケーションを識別する。この説明は、発行者のサーバー３０９に送られるアプリケーション・キー・プロキシ３１１と関連している。発行者のサーバー３０９は、ユーザを認証

16

した上で、アプリケーションのロケーションと、それにアクセスするために使用される本物かつ実際の鍵を参照する。次に、発行者のサーバーは消費者をアプリケーションサーバー３１３のアプリケーションに導き、セキュアコンジットとして機能する。

【００５４】すでにお分かりのように、カードを紛失または盗まれた場合に、プロキシは実際の鍵の代わりに用いられる。このように、新たな鍵を発行するために多くのつながりのない組織と協調を保つ必要はなくなる。発行者は単に、新たなプロキシを乗せた新たなカードを発行するだけでよい。

【００５５】以下、添付の図面において開示したような本発明の多数の異なる特徴について述べる。全てのフローチャートにおいて、システムの各コンポーネントは一番上の水平軸に沿って識別され、各ステップの説明は左側の垂直軸に沿って識別されている。さらに、チャートの中程には一部単語である矢印が含まれており、システムのコンポーネント間での相互作用および情報の流れを示している。両頭矢印は対話の流れが双方向であることを示し、通常はレベルが低くなるほどより詳細な対話（図示せず）が起こっている。

【００５６】これらのフローチャートに示すステップは、仮想ウォレットのユーザによって実施されるか、あるいはパーソナル格納装置、インタフェースまたは団体のサーバーに置かれているコンピュータソフトウェアにおいて実現される。

【００５７】－仲介されたトランザクション－

図５を参照すると、本発明の１つの特徴は、ウォレットサーバーを利用して仮想ウォレットと店主との間のトランザクションを監督する。例えば、ウォレットの所有者は店主の位置でショッピングをすることができる。ウォレットの所有者は仮想ウォレットを利用してアイテムを購入することを決める。仮想ウォレットを利用して、所有者は購入要求を店主に送信する。店主のサーバーなどの店主の装置は、購入要求を受信し、ウォレットの所有者が購入したいと思っているアイテムを確認し、ウォレットのサーバーを介してウォレットの所有者に支払い要求を送信する。これらの要求は、例えばマルチメディア・インターネット・メール拡張仕様（ＭＩＭＥ）フォーマットなどで送信することができる。次にウォレットのサーバーは要求を請求書の形でブラウザまたは他の同様のアプリケーションなどのウォレットのインタフェースに転送する。請求書は、例えば、購入オーダー情報および受領支払いメカニズムからなる情報のパッケージである。さらに、これがインターネットでのトランザクションである場合には、請求書は例えば獲得者のサーバーへのＵＲＬも含んでもよい。請求書の受領時、ウォレットの所有者は請求書を見て、支払い方法を選択し、請求書の受領書に署名をする。署名のある受領書および選択した支払いメカニズムはウォレットのサーバーに戻り、こ

れによって支払いトランザクションが仲介される。例えば、ウォレットのサーバーはSecure Electronic Transaction(SET)プロトコルまたは同様のトランザクションプロトコルを利用して、ウォレットの所有者のアカウント番号、支払い金額、応諾などの支払い情報を交換することができる。次に、最終的な応諾または拒否がウォレットの所有者のもとへ送られる。最後に、実現メカニズム（図示せず）が開始され、ウォレットの所有者に受領させてトランザクションを完了させなければならない。

【００５８】－支払い用ウォレットオープン－

図６は、ウォレットが支払い用に開かれ、ウォレットのサーバーによって支払い要求が受領される特徴を表す。支払い要求は、例えばＳＥＴ開始ＭＩＭＥ、ＪＣＭ（ＪＡＶＡ取引メッセージ）およびオープン・トレーディング・プロトコル（ＯＴＰ）などのいかなる形式のものであってもよい。ウォレットが開くと、ウォレットの所有者またはユーザはウォレットに対して自分たちを認証させ、正しいユーザがウォレットのインタフェースを使用していることをウォレットに知らせなければならない。ユーザは、バイオメトリック情報、ＰＩＮおよびパスワード、または他の同様の方法を利用して自己を認証させることができる。一旦ユーザを認証してしまえば、ウォレットおよびウォレットのサーバーは相互に相手を認証しなければならない。様々な認証が完了すると、支払い要求から発生した請求書および支払いメカニズムがウォレットのサーバーを介してウォレットの所有者に提示される。ウォレットの所有者はウォレットインタフェースのディスプレイを介して情報を見て、ウォレットのサーバーを介して選択した支払手段を送り返す。

【００５９】次に、ウォレットのサーバーは、ウォレットの所有者によって署名するための特別な支払い応諾許可オブジェクトを有利にウォレットの所有者に与える。伝統的には、一度支払いが承知されると文書にデジタル署名が自動的に添付される。しかしながら、本発明のかかる任意の特徴では、ウォレットの所有者は意識的に請求書または受領書に署名をするステップに進む。デジタル署名などの応諾許可を獲得するための方法を提供することもできる。

【００６０】最後に、署名された文書はウォレットのサーバーによって処理される。ウォレットのサーバーは、ＳＥＴまたは他の同様のプロトコルなどの適当なプロトコルを利用して支払いトランザクションを開始し、これを仲介する。

【００６１】上述したように、デジタル書類をフォーマットして送出するための方法は様々な形を取り得る。例えば、１つの好ましいフォーマットは拡張可能なマークアップ言語（ＸＭＬ）である。これは他の言語のフォーマットを記述するのに使用されるメタ言語である。コンピュータからコンピュータへ移動可能なのは構造化された形のデータフォーマットを組織化する方法である。同



様に、フォーマットはオブジェクトの形でのＪａｖａであってもよいし、あるいは、フォーマットは状態と挙動を要約する比較的標準的な他の方法であってもよい。

【００６２】－公開鍵発行－

図７を参照すると、本発明の他の有利な特徴は、公開／秘密鍵のペアを生成し、発行し、インデックス化することである。本発明の仮想ウォレットシステムの利点は、ローカルな態様が公開／秘密鍵のペアを生成できるという点である。公開鍵をウォレットのサーバーに対して発行し、一方秘密鍵をローカルに残しておいてもよい。この特徴によって、消費者が秘密鍵だけを持っている場合に非支払い拒絶を保護しやすくなる。ローカルな置き場（クライアント）がスマートカードである好ましい実施態様では、秘密鍵がスマートカードから離れることは決してない。

【００６３】この公開鍵発行特徴によって、第三者の証明書無効リスト（ＣＲＬ）をチェックしなければならないこととは対照的に、署名された文書を信頼して鍵を発行する当事者がその有効性をチェックすることができるようになる。この場合、ウォレットの所有者はウォレットに新しい鍵のペアを生成するよう頼む。あるいは、これは要求されるソフトウェアの一部であってもよい。しかしながら、いずれの場合でも、複数のアクティブな鍵のペアが存在することもある。チップ装置は、処理終了後、公開鍵を返してウォレットのサーバーからこれを関連させるインデックスを要求する。ウォレットのサーバーは公開鍵およびインデックス要求を公開鍵ディレクトリに転送する。ここで、２つの異なるエンティティすなわちウォレットのサーバーおよび公開鍵ディレクトリが存在することもあると仮定されるが、これらは同一の法人下にあることができる。公開鍵ディレクトリは鍵を発行し、本発明の独特な特徴によれば、この鍵に対するインデックスをウォレットのサーバーに返す。ウォレットのサーバーは、これを受けて、複製をチップ装置に返す。次に、チップ装置は、鍵の発行およびインデックスの受領をウォレットの所有者に対して確認する。

【００６４】インデックスは意味の分からない数字の羅列であることがあるため、本発明は有利に、ウォレットの所有者がインデックスと「親しみのある名前」またはニックネームとを関連付けられるようにしている。ウォレットの所有者が、異なる個人に対してあるいは異なる関係について複数の署名鍵を有していることもあるため、所有者が覚えやすい名前をそれぞれの鍵のインデックスに対して作成できるというのは重要なことである。最後に、チップ装置は鍵と一緒にインデックスを安全に格納して将来の使用に備える。

【００６５】－デジタル文書への署名－

署名を操作するにあたり、レストランなどの要求者はウォレットの所有者に対して受領書などの書類に署名するよう望む。要求者は対話を開始し、文書をウォレットに

送信する。ウォレットは文書をソフトウェアによって認識するための署名文書として指定する。ウォレットのサーバーは、署名文書がオンラインに来るとこれをウォレットのインタフェースに送信することによって、同期対話および非同期対話の両方をサポートする。ウォレットのインタフェースは署名文書およびアブストラクトをウォレットの所有者に対して表示して署名を求める。次に、所有者は自分の署名鍵ニックネームのうちの１つすなわち、換言すれば、署名をする相手をを抽出し、文書に署名する。本発明のかかる特徴は、複数の署名鍵を有利に管理する。

【００６６】－クーポンでの購入－

本発明のかかる機能は、図８を参照すると、ウォレットの所有者のためにクーポンを集め、ウォレットの所有者が支払い要求請求書を提示された時に適当なクーポンを比較して選択するクーポン管理システムを有利に提供する。このシステムには、所有者が個々のトランザクションに対して適用されるクーポン全てを一度に選択し、まとめて買い戻すことができるようにするという利点がある。

【００６７】この場合、ウォレットの所有者は店主のところで買い物をし、購入するアイテムを示した後、店主のサーバーが支払い要求と可能な支払手段のリストとをウォレットの所有者に送信する。支払い要求は請求書も含み、請求書のオブジェクトには請求書に含まれているアイテムおよび品番が分かっている。請求書のオブジェクトはそのリストをクーポンマネジャーに送り、クーポンマネジャーが請求書を分析し、ウォレットの所有者が保持しているクーポンを含むクーポンリストと比較する。一致するものが見つかったら、クーポンマネジャーは適切なクーポンのリストを作成し、このリストをウォレットの所有者に提示する。リストは、好ましくは全てが一度に提示されるが、適切なクーポン各々を１度に１つずつ交互に提示してもよい。所有者はどのクーポンを使用するか示し、クーポンマネジャーが示されたクーポンのリストをディスカウント要求として店主のサーバーに返す。受信したクーポンに基づいて、店主は請求書を更新し、店主のサーバーが更新後の支払い要求を所有者に返す。ウォレットの所有者は支払いメカニズムを選択して支払い要求に署名をする。これが店主に転送される。最後に、店主が従来の手段を介して支払いの応諾許可を得ようとし、所有者に対して応諾許可を得ようとした結果を通知する。

【００６８】さらに、クーポンマネジャーは、請求書に列挙されているアイテムの代わりになるものあるいはこれと等価なものであるアイテムに対するクーポンを持っていることを理由に、所有者に対して他の物を購入することを提案する。さらに、店主は、等価または代わりのアイテムに対して、あるいは最初に示されたアイテムにですらクーポンを提供し、所有者に対してクーポンプレ



ゼントオプションを与えることもできる。いずれの場合も、クーポンマネジャーはこれらのオプションを所有者の承認を得るよう提示する。

【００６９】－チケット購入および使用－

図９を参照すると、本発明のさらに他の特徴では、ウォレットの所有者が、チケット、トークンまたは他の類似の転送可能な有価アイテムを購入、格納および使用することができる。チャートにおいて線と線との間の空間は、時間の経過を示す。この場合、例えば、所有者は劇場に働きかけてショーのチケットを購入しようとする。劇場のサーバーは、支払いを応諾許可する所有者からの支払いを要求する。劇場側で支払いを確認後、劇場のサーバーはウォレットのサーバーにチケットを送信し、このサーバーがチケットを後に使用できるよう格納する。チケットは移送されるオブジェクトであり、１つの場所から他の場所に転送可能である。所有者がチケットをローカルに格納しておくことを決めた場合には、所有者はウォレットのサーバーに対してチケットをローカルに格納するよう要求する。次にチケットオブジェクトは、スマートカードなどのセキュアチップ装置に転送される。劇場に到着したら、劇場のサーバーがチケットを要求し所有者はチップ装置をウォレットのインタフェースに差し込んでチケットにアクセスするか、あるいは、劇場のインタフェースにアクセスする。所有者は、相互の認証プロセスを経た後に劇場のサーバーにチケットが転送されると、劇場に入ることを許可される。

【００７０】本発明の他の態様、特徴および利点および作用を以下の実施例において説明する。

【００７１】－実施例－

以下、仮想ウォレットおよびこれを取引において使用することについての実施態様の実施例を図１０および図１１を参照して説明する。

【００７２】ハイブリッドウォレットは、物理的にユーザの手元にあるスマートカードとサーバーベースのウォレットとの組み合わせである。このためウォレットは、オフラインおよびオンラインの両方で適切なタスクを行うよう機能できるようにする３つの異なるアプリケーションを有する。

【００７３】第１のエリアは格納値エリアまたはがまロである。このエリアは、オフラインで電子キャッシュを分配して追跡することができ、オンラインで再ロード可能である。

【００７４】第２のエリアは本質的に現在のカードの磁気ストリップと等価なものであるが、物理的なカードをウォレットに収容されている他のあらゆるカードに対するプロキシとすることができるようにしている。これによって、ユーザが物理的な店舗にいる場合に既存のチャネルを利用しての購入が可能になる。カードを交換しなければならない場合にはアカウント情報はサーバー上にミラーとして保持される。

【００７５】第３のエリアは、電子ウォレットの「残りの部分」を示し、単純に保持者がサーバー上のウォレットにアクセスできるようにする資格である。このような資格は、暗号文（ｃｒｙｔｏｇｒａｍ）、証明書、署名入りの記録（ｉｎｄｉｃａ）などの形であることもできる。これによって、実際のカードリソースが極めて限られている場合に多くのウォレットアイテムを持つ能力が提供される。さらに、消費者のマシンとサーバーとの間で通常発生するよりも高い帯域幅で高速サーバーとの間で通信が起こるため、全体としての性能が改善される。

【００７６】さらに、カードを紛失したり、カードが盗難または災害に遭ったりした場合に、古い資格を無効にして新たなものが容易に再発行される。例えば、各ウォレットアイテムが各ウォレットアイテム（アプリケーション）業者から各々証明書を発行してもらう必要のある最悪の事態のシナリオを想定する。スマートカード上の全資格が盗まれた場合、各業者に連絡をし、カードが悪用される前にカードを無効にして再発行してもらわなければならない。資格をサーバーに格納しておくことで、このような複雑な問題は回避され、ウォレットの発行者が制御を有する１つの証明書すなわちネットワークウォレットへの証明書を無効にして再発行する単純なタスクに置き換えることができる。ウォレットのユーザにとっては中身が実際にどこにあるかは明らかではないこともある。仮想ウォレットはその中身を全て一緒に持っているように見える。

【００７７】しかしながら、中身の実際の物理的な配布は、オフラインで利用できなければならないものと、サーバーに置いておくことのできるものとによって決められる。図１０および１１は、オフライン（インターネット上ではない）トランザクション向けのスマートカード上の機能のいくつかと、ネットワーク上の仮想ウォレットの残りにアクセスするための１つの証明書とを示している。

【００７８】図１０は仮想ウォレットの中身を示すブロック図である。図１０に示されるように、仮想ウォレットの所有者は、ウォレットを用いて、クレジットカードおよびキャッシュカードの他、関連の金融情報を保持（収容）することができる。この金融通貨には、本実施例では、ＶＩＳＡ（登録商標）キャッシュ１２２と、ＶＩＳＡ（登録商標）証明書１２４と、ＶＩＳＡ（登録商標）クレジットカード１２６と、ＭａｓｔｅｒＣａｒｄ（登録商標）クレジットカード１２８と、Ｍｏｎｄｅｘクレジット１３０と、Ｍｏｎｄｅｘ証明書１３２と、Ｄｉｎｅｒｓ　Ｃｌｕｂクレジットカード１３４と、ＭａｓｔｅｒＣａｒｄ（登録商標）ＳＥＴ証明書１３６と、ＶＩＳＡ（登録商標）ＳＥＴ証明書１３８と、Ｄｉｎｅｒｓ　ＳＥＴ証明書１４０とが含まれている。金融通貨はさらに、例えばＣｉｔｉ　Ｓｈｏｐｐｉｎｇ　Ｎｅｔｗｏｒｋ　Ｃｒｅｄｉｔｓ１４２およびガソリン会社のクレジット１４４などの選択した業者からのクレジットを含んでもよい。さらに、ウォレット１２０はマイレージポイント１４６などの報償プログラム情報を含んでもよい。金融通貨に加えて、仮想ウォレット１２０は所有者に関連している「情報」通貨も含んでいる。情報通貨の例としては、電話番号簿１４８、カレンダーおよびスケジュール帳１５０、身元確認情報１５２、懸案事項リスト１５４、テレフォンカード１５６、個人情報１５８、個人の興味の内容１６０およびネットワークウォレット身元確認証明書１６２が挙げられる。



【００７９】図１１は、本実施例の仮想ウォレット１２０の物理的な実施例を示す。図１１に示されるように、仮想ウォレットはスマートカード１７０とウォレットのサーバー１７２との間のハイブリッドである。スマートカード１７０は、ＶＩＳＡ（登録商標）キャッシュ１２２と、ＶＩＳＡ（登録商標）ＳＥＴ証明書１３８と、ＶＩＳＡ（登録商標）証明書１２４と、ＶＩＳＡ（登録商標）クレジットカード１２６と、Ｍｏｎｄｅｘクレジット１３０と、Ｍｏｎｄｅｘ証明書１３２と、ネットワークウォレット身元確認証明書１６２とを含んでいる。ウォレットのサーバー１７２は、ＭａｓｔｅｒＣａｒｄ（登録商標）クレジットカード１２８と、Ｄｉｎｅｒｓ　Ｃｌｕｂクレジットカード１３４と、ＭａｓｔｅｒＣａｒｄ（登録商標）ＳＥＴ証明書１３６と、Ｄｉｎｅｒｓ　ＳＥＴ証明書１４０と、電話番号簿１４８と、カレンダーおよびスケジュール帳１５０と、身元確認情報１５２と、懸案事項リスト１５４と、テレフォンカード１５６と、個人情報１５８と、Ｃｉｔｉ　Ｓｈｏｐｐｉｎｇ　Ｎｅｔｗｏｒｋ　Ｃｒｅｄｉｔｓ１４２と、ガソリン会社のクレジット１４４と、マイレージポイント１４６と、個人の興味の内容１６０とを含んでいる。

【００８０】図１１に概略的に示すように、仮想ウォレット１２０の所有者はスマートカード部分１７０を使用して電子キャッシュトランザクション１８０を完了し、例えばタクシー料金１８２を支払ってもよい。また、スマートカード１７０をクレジットカードトランザクション１８４および１８６において利用してもよい。また、スマートカード１７０は、サーバー１７２またはインターネット１９０を介してのウォレットのネットワーク部分へのプロキシ１８８でもある。通行インタフェースによって、ユーザは、まるでスマートカード上にあるかのようにウォレットのサーバー上のアプリケーションからアイテム（情報または金融通貨）を選択することができる。アプリケーションおよび通貨はサーバー上に常駐しているため、スマートカードのメモリの大きさに数が制約されることはなく、カードが悪用された場合などに容易にカードを交換できる。

【００８１】さらに別の機能は、仮想ウォレット１２０のウォレットのサーバー１７２部分によって提供される。ウォレットのサーバー、あるいはウォレットのサー

バーへのインタフェースを介したスマートカードは、インターネットを介して店主のサーバー１９２と通信をし、商品または金融サービスを購入したり、あるいは情報を交換したりすることができる。

【００８２】仮想ウォレット１２０の特徴は、Ｊａｖａ Ｗａｌｌｅｔ ＭｏｄｅｌおよびＪａｖａ Ｅｌｅｃｔｒｏｎｉｃ Ｃｏｍｍｅｒｃｅ Ｆｒａｍｅｗｏｒｋ（ＪＥＣＦ）を利用して実現可能である。ＪＥＣＦは、一組の取引用Ｊａｖａ ＡＰＩである。ＪＥＣＦは取引メッセージおよびオペレーションについてのオブジェクトを定義する。代表的なスキームを図１２に示しておく。

【００８３】図１２に示されるように、ＪＥＣＦは、オペレーションレジストリ２００と、プロトコルレジストリ２０２と、ユーザインタフェース（ＵＩ）レジストリ２０４と、機器レジストリ２０６と、機器例２０８とを含んでいる。オペレーションレジストリは、例えばカードからの値を加算または減算するなどのオペレーションをサポートする。プロトコルレジストリは、クレジットカードの支払い応諾許可のようなオペレーションを実施する、ＳＥＴなどのプロトコルをフレームワークに含ませることができるようにする。機器レジストリは、通信用の基本的なプロトコルを使用する、格納された有価カードまたはクレジットカードなどの金融機器をサポートする。機器は自分がサポートされているものを複数のプロトコルの中から選択してもよい。ＵＩレジストリは、異なるユーザインタフェース間でフレームワークを切り換え、基本的なオペレーションのベースセットを制御できるようにする。また、オブジェクト間での通信用にセキュリティモデルも包含されている。

【００８４】ＪＥＣＦ内での指示の流れは、一例として、以下のようになる。ｊａｖａ取引メッセージ（ＪＣＭ）がＪＥＣＦに入力される。ＪＥＣＦはオペレーション（必要であれば、コンポーネントをダウンロードする）を参照してそれを例示する。ＪＥＣＦは、オペレーションに関連した現在のユーザインタフェースを参照し、そのユーザインタフェースを表示する。ＪＥＣＦはオペレーションをユーザインタフェースに追加し、ユーザによってオペレーションが終了されるのを待つ。ユーザは、ユーザインタフェースと相互作用しながらオペレーションを実施する。オペレーションが完了すると、ストリング応答が返され、これがオペレーションの呼び手に返される。



【００８５】仮想ウォレット１２０においてＪＥＣＦの機能を他のソフトウェアと一緒に利用して、先のセクションにおいて上述したような機能を実施することもできる。

【００８６】以上、好ましい実施態様および特徴を参照して本発明を説明したが、同様の実施態様および特徴でも同一の結果を達成することができる。本発明を変形および修正したものは当業者には明らかであり、本願の開示はかかる修正物および等価なものを全て包含するものとする。

【図面の簡単な説明】

【図１】本発明の仮想ウォレットシステムの一実施態様の概略図である。

【図２】本発明の仮想ウォレットシステムの一実施態様の他の概略図である。

【図３】本発明による電子ウォレットアーキテクチャの一実施態様の概略図である。

【図４】本発明による電子ウォレットアーキテクチャの一実施態様の他の概略図である。

【図５】本発明の仲介トランザクション機能のフローチャートである。

【図６】本発明の支払い用ウォレットオープン機能のフローチャートである。

【図７】本発明の公開鍵発行機能のフローチャートである。

【図８】本発明のクーポンでの購入機能のフローチャートである。

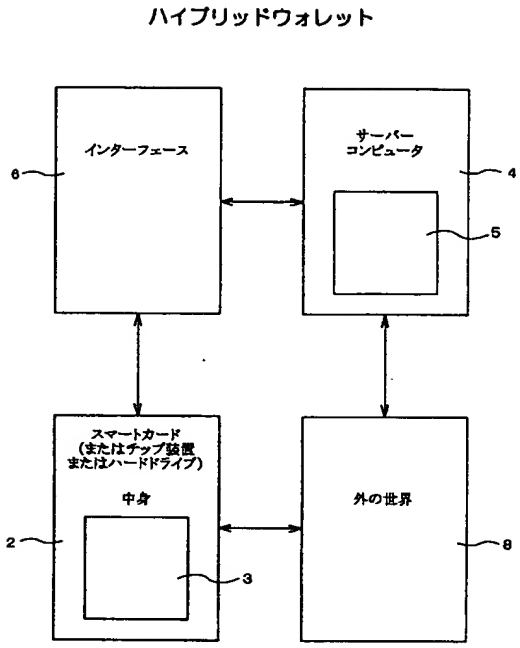
【図９】本発明のチケット購入および使用機能のフローチャートである。

【図１０】本発明の仮想ウォレットの一例の中身の概略図である。

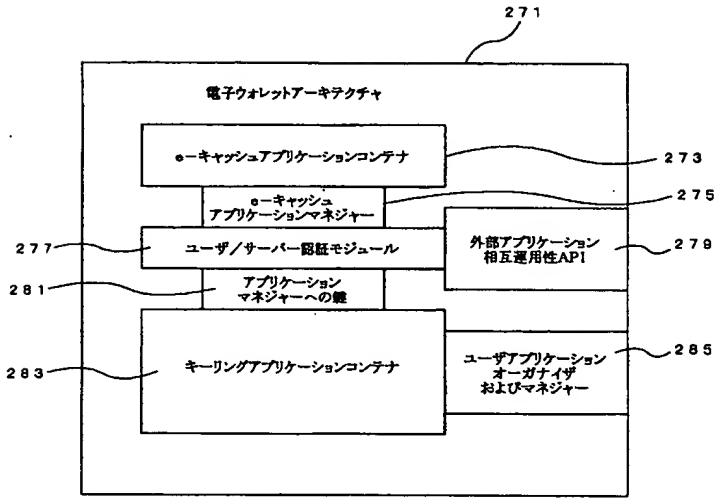
【図１１】本発明の仮想ウォレットシステムの一例を示す図である。

【図１２】本発明の仮想ウォレットシステムの一例において利用可能なＪＡＶＡ ＡＰＩの概略図である。

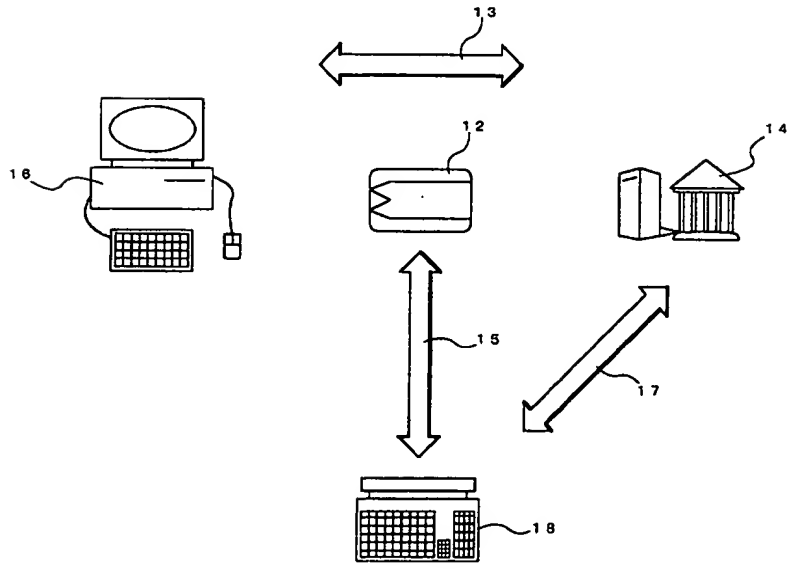
【図１】


ハイブリッドウォレット
インターフェース
6
サーバー
コンピュータ
4
5
スマートカード
(またはチップ装置
またはハードドライブ)
中身
2
3
外の世界
8

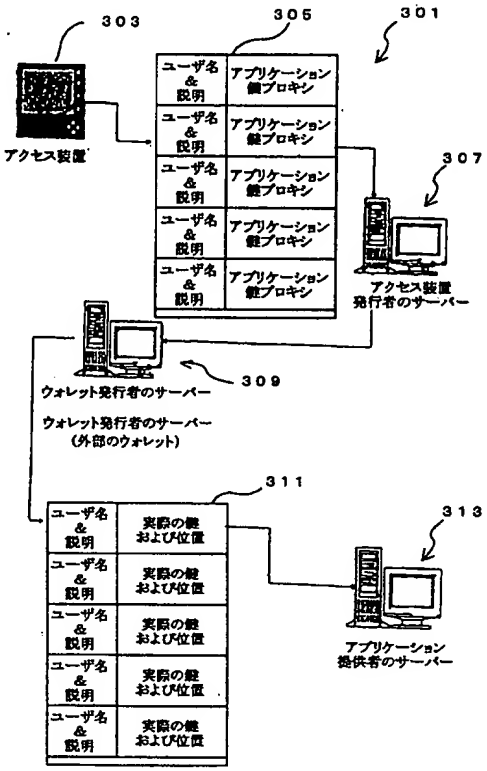
【図３】


271
電子ウォレットアーキテクチャ
e-キャッシュアプリケーションコンテナ
273
e-キャッシュ
アプリケーションマネジャー
275
277
ユーザ/サーバー認証モジュール
外部アプリケーション
相互運用性API
279
281
アプリケーション
マネジャーへの鍵
283
キーリングアプリケーションコンテナ
ユーザアプリケーション
オーガナイザ
およびマネジャー
285

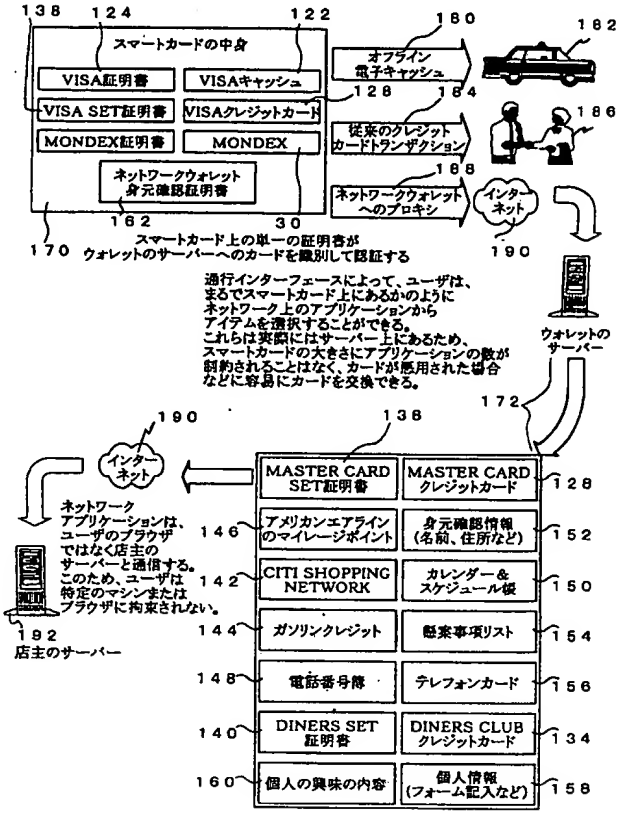
【図２】


13
12
14
16
15
17
18

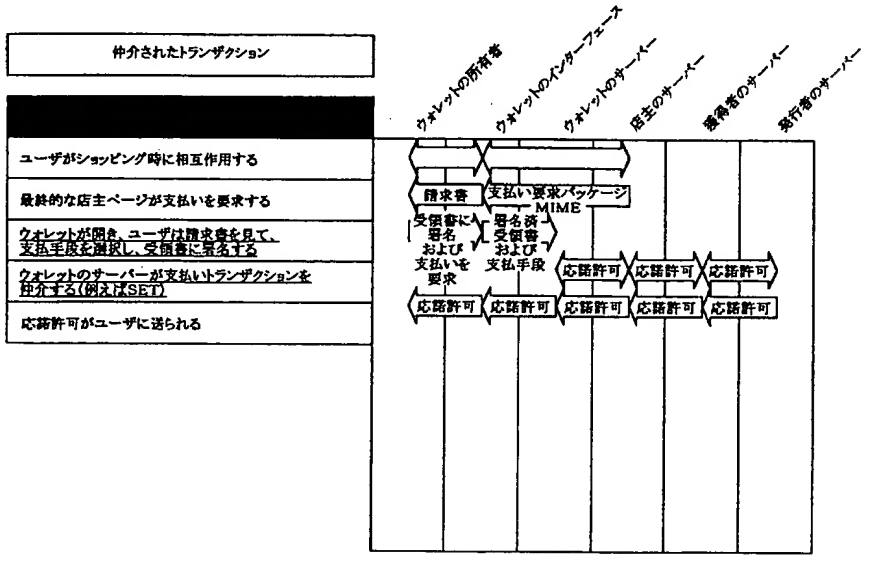
【図４】


303
305
301
307
309
311
313
アクセス装置
ユーザ名 & 説明
アプリケーション鍵プロキシ
アクセス装置発行者のサーバー
ウォレット発行者のサーバー
ウォレット発行者のサーバー（外部のウォレット）
実際の鍵および位置
アプリケーション提供者のサーバー

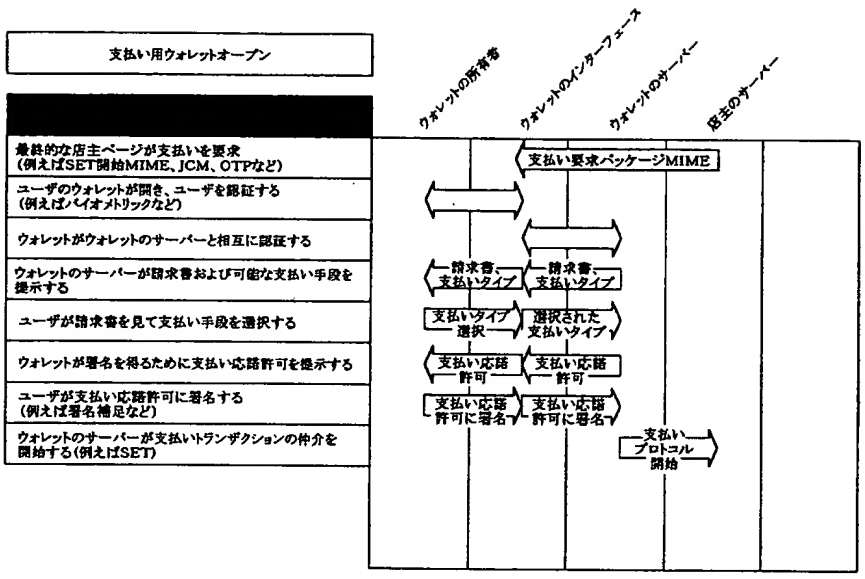
【図１１】


138
124
122
スマートカードの中身
VISA証明書
VISAキャッシュ
VISA SET証明書
VISAクレジットカード
MONDEX証明書
MONDEX
ネットワークウォレット身元確認証明書
162
30
170
スマートカード上の単一の証明書がウォレットのサーバーへのカードを識別して認証する
180
オフライン電子キャッシュ
182
128
184
186
従来のクレジットカードトランザクション
188
ネットワークウォレットへのプロキシ
インターネット
190
ウォレットのサーバー
通行インターフェースによって、ユーザは、まるでスマートカード上にあるかのようにネットワーク上のアプリケーションからアイテムを選択することができる。これらは実際にはサーバー上にあるため、スマートカードの大きさにアプリケーションの数が制約されることはなく、カードが悪用された場合などに容易にカードを交換できる。
172
MASTER CARD SET証明書
MASTER CARD クレジットカード
アメリカンエアラインのマイレージポイント
身元確認情報（名前、住所など）
CITI SHOPPING NETWORK
カレンダー＆スケジュール帳
ガソリンクレジット
懸案事項リスト
電話番号簿
テレフォンカード
DINERS SET 証明書
DINERS CLUB クレジットカード
個人の興味の内容
個人情報（フォーム記入など）
ネットワークアプリケーションは、ユーザのブラウザではなく店主のサーバーと通信する。このため、ユーザは特定のマシンまたはブラウザに拘束されない。
192
店主のサーバー

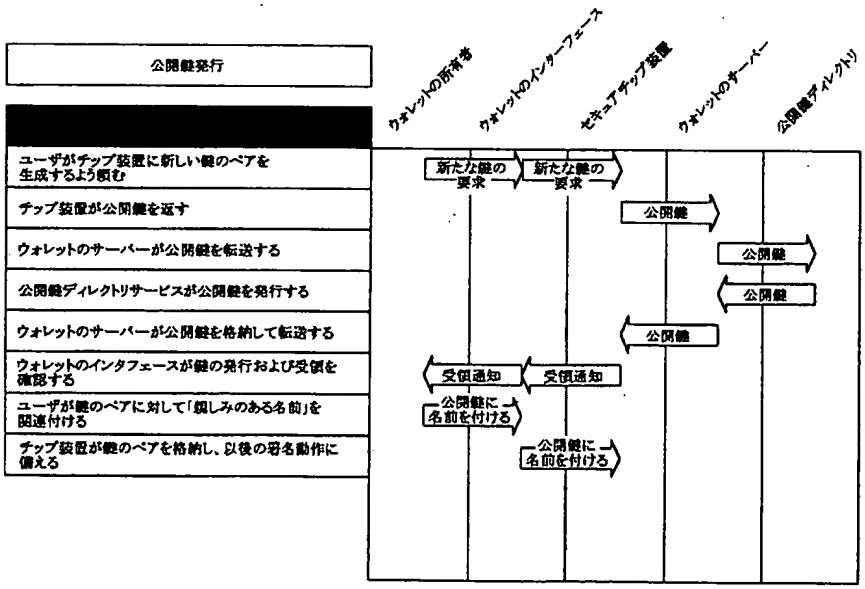
【図５】


仲介されたトランザクション
ユーザがショッピング時に相互作用する
最終的な店主ページが支払いを要求する
ウォレットが開き、ユーザは請求書を見て、支払手段を選択し、受領書に署名する
ウォレットのサーバーが支払いトランザクションを仲介する（例えばSET）
応諾許可がユーザに送られる
ウォレットの所有者
ウォレットのインターフェース
ウォレットのサーバー
店主のサーバー
銀行者のサーバー
発行者のサーバー
請求書
支払い要求パッケージ
MIME
受領書に署名および支払いを要求
署名済受領書および支払手段
応諾許可

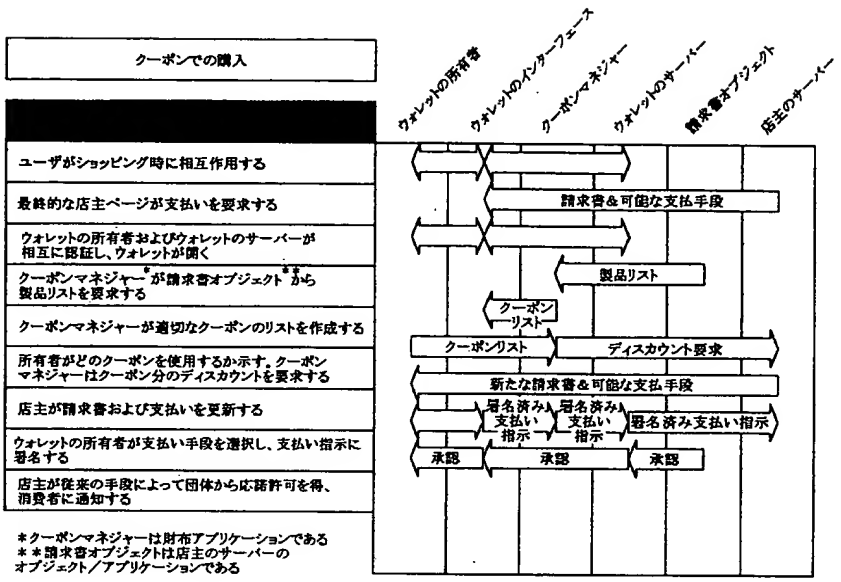
【図６】


支払い用ウォレットオープン
最終的な店主ページが支払いを要求
(例えばSET開始MIME、JCM、OTPなど)
ユーザのウォレットが開き、ユーザを認証する
(例えばバイオメトリックなど)
ウォレットがウォレットのサーバーと相互に認証する
ウォレットのサーバーが請求書および可能な支払い手段を提示する
ユーザが請求書を見て支払い手段を選択する
ウォレットが署名を得るために支払い応諾許可を提示する
ユーザが支払い応諾許可に署名する
(例えば署名補足など)
ウォレットのサーバーが支払いトランザクションの仲介を開始する(例えばSET)
ウォレットの所有者
ウォレットのインターフェース
ウォレットのサーバー
店主のサーバー
支払い要求パッケージMIME
請求書、支払いタイプ
請求書、支払いタイプ
支払いタイプ選択
選択された支払いタイプ
支払い応諾許可
支払い応諾許可
支払い応諾許可に署名
支払い応諾許可に署名
支払いプロトコル開始

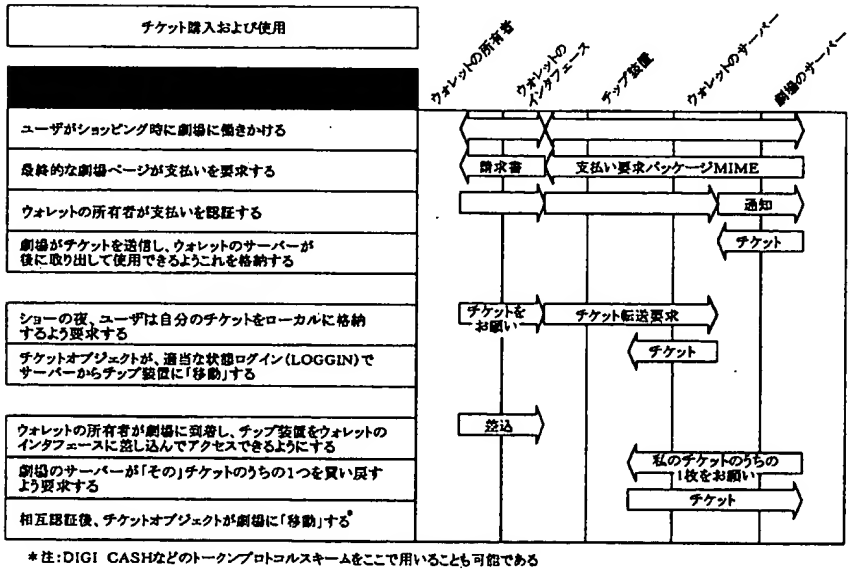
【図７】


公開鍵発行
ユーザがチップ装置に新しい鍵のペアを生成するよう頼む
チップ装置が公開鍵を返す
ウォレットのサーバーが公開鍵を転送する
公開鍵ディレクトリサービスが公開鍵を発行する
ウォレットのサーバーが公開鍵を格納して転送する
ウォレットのインタフェースが鍵の発行および受領を確認する
ユーザが鍵のペアに対して「親しみのある名前」を関連付ける
チップ装置が鍵のペアを格納し、以後の署名動作に備える
ウォレットの所有者
ウォレットのインターフェース
セキュアチップ装置
ウォレットのサーバー
公開鍵ディレクトリ
新たな鍵の要求
新たな鍵の要求
公開鍵
公開鍵
公開鍵
公開鍵
受領通知
受領通知
公開鍵に名前を付ける
公開鍵に名前を付ける

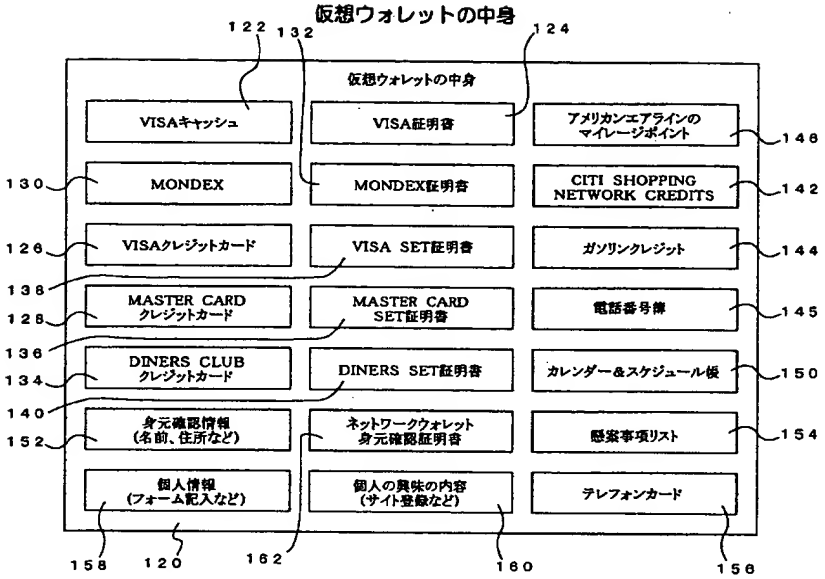
【図８】


クーポンでの購入
ユーザがショッピング時に相互作用する
最終的な店主ページが支払いを要求する
ウォレットの所有者およびウォレットのサーバーが相互に認証し、ウォレットが開く
クーポンマネジャー*が請求書オブジェクト**から製品リストを要求する
クーポンマネジャーが適切なクーポンのリストを作成する
所有者がどのクーポンを使用するか示す。クーポンマネジャーはクーポン分のディスカウントを要求する
店主が請求書および支払いを更新する
ウォレットの所有者が支払い手段を選択し、支払い指示に署名する
店主が従来の手段によって団体から応諾許可を得、消費者に通知する
*クーポンマネジャーは財布アプリケーションである
**請求書オブジェクトは店主のサーバーのオブジェクト／アプリケーションである
ウォレットの所有者
ウォレットのインターフェース
クーポンマネジャー
ウォレットのサーバー
請求書オブジェクト
店主のサーバー
請求書＆可能な支払手段
製品リスト
クーポンリスト
クーポンリスト
ディスカウント要求
新たな請求書＆可能な支払手段
署名済み支払い指示
署名済み支払い指示
署名済み支払い指示
承認
承認
承認

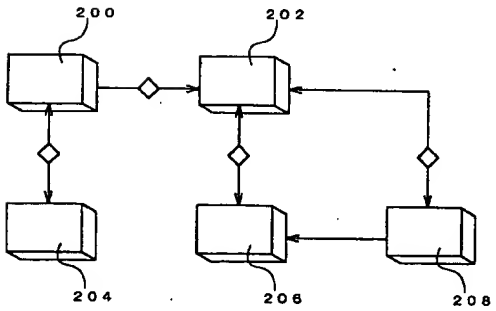
【図９】


チケット購入および使用
ユーザがショッピング時に劇場に働きかける
最終的な劇場ページが支払いを要求する
ウォレットの所有者が支払いを認証する
劇場がチケットを送信し、ウォレットのサーバーが後に取り出して使用できるようこれを格納する
ショーの夜、ユーザは自分のチケットをローカルに格納するよう要求する
チケットオブジェクトが、適当な状態ログイン(LOGGIN)でサーバーからチップ装置に「移動」する
ウォレットの所有者が劇場に到着し、チップ装置をウォレットのインタフェースに差し込んでアクセスできるようにする
劇場のサーバーが「その」チケットのうちの1つを買い戻すよう要求する
相互認証後、チケットオブジェクトが劇場に「移動」する*
*注：DIGI CASHなどのトークンプロトコルスキームをここで用いることも可能である
ウォレットの所有者
ウォレットのインタフェース
チップ装置
ウォレットのサーバー
劇場のサーバー
請求書
支払い要求パッケージMIME
通知
チケット
チケットをお願い
チケット転送要求
チケット
差込
私のチケットのうちの1枚をお願い
チケット

【図１０】




【図１２】




フロントページの続き

| (51) Int. Cl.[6] | 識別記号 | FI | |
|---|---|---|---|
| | | G06F 15/30 | 350A |
| | | G07D 9/00 | 476 |

(71)出願人 598156527
12731 W. Jefferson Boulevard, Los Angeles, California 90066, U. S. A.
(72)発明者 アルノール ビー. マムダーニ
アメリカ合衆国 カリフォルニア州 90291, ヴェニス, ペンマー アヴェニュー 2030
(72)発明者 チャールス ゴルヴィン
アメリカ合衆国 カリフォルニア州 90064, ロス アンジェルス, マコーネル ドライヴ 2762
(72)発明者 ヘンリー リクステイン
アメリカ合衆国 カリフォルニア州 90402, サンタ モニカ, ドュライド ロード 544
(72)発明者 ディビッド ソロ
アメリカ合衆国 ニューヨーク州 10021, ニューヨーク, セブンティフィフス ストリート 300 イー., アパートメント 7Ｂ
(72)発明者 ジャック パン
アメリカ合衆国 カリフォルニア州 91748, ロウランド ヘイツ, サウス ノウィック プレイス 3651
(72)発明者 メルヴィン エム. タカタ
アメリカ合衆国 カリフォルニア州 91360, サウザンド オークス, パセオ デル ロブレード 855

【外国語明細書】

# VIRTUAL WALLET SYSTEM

## Cross-reference to Related Applications

The present application claims priority under 35 USC 119(e) from US Provisional Patent Application No. 60/065,291 entitled "DISTRIBUTED NETWORK BASED ELECTRONIC WALLET," filed November 12, 1997 and from US Provisional Patent Application No. 60/081,748 entitled "VIRTUAL WALLET SYSTEM" filed April 14, 1998. The disclosures of each referenced application is hereby incorporated herein by reference.

## Field of the Invention

The present invention relates to apparatus, systems and methods for information and financial banking. Particular features of the present invention include electronic wallets and computer and related electronic apparatus based systems for the storage, retrieval and management of personal information including personal financial information. An additional feature of the present invention is a system for a digitized signature.

## Background

With the explosion in popularity and utility of the internet and other electronic transaction mediums, the need for and dependence upon information in an electronic format is ever-increasing. The problem of storing, retrieving and managing all of a consumer's electronic data, however, has not yet been satisfactorily analyzed or solved.

Further, the problem is not currently being approached from the consumer's standpoint, but from the standpoint of the vendor looking to solve particular vendor needs. One form of product that deals with some of the above-stated needs are generally called electronic wallets. Typically, current electronic wallets are just an afterthought, however, used by vendors to enhance other products. Generally, an electronic wallet is a software application, on a network or within a browser, that is part of a much larger program. Electronic wallets focus primarily upon the payment

aspects of electronic commerce. For example, electronic wallets comprise credit card account information and digital certificates that are used in authorizing electronic transactions that can be performed with the main product sold by the vendor.

Additionally, electronic wallets are typically not universally interoperable. Information added to the electronic wallet application of one vendor may not be able to be used by or accessed from other applications. In fact, a vendor providing a program may require that only the electronic wallet application associated with that program be used. Thus, a consumer is presented with the frustrating task of repeatedly entering and acquiring the data and information necessary to build the components of their electronic wallet.

Further, because current electronic wallets are primarily designed as a part of a bigger application, they typically have narrow functionality. Current electronic wallets generally are only able to hold certain pre-designated types of electronic information, such as credit card account information or digital certificates. Typically, applications utilizing current electronic wallets may only need a payment function, and thus the electronic wallet only provides this function. Generally, the functionality of current electronic wallets is driven by vendor, rather than consumer, needs. On the other hand, a consumer looking to integrate an electronic wallet into all facets of their life needs the ability to store, manage and retrieve varied data from multiple data sources. Thus, there is a need for an electronic wallet that is able to work with electronic data that is chosen based on the electronic wallet owner's needs, not just the needs of a particular software vendor.

Additionally, electronic wallets typically reside either locally with the owner, such as in a smart card or on a personal computer, or remotely such as on a server. There are drawbacks to both residences.

Local residence has the advantage of complete control by the owner and not much resource allocation required by virtual wallet issuer. On the other hand, the local residence of an electronic wallet exposes the owner to the greatest risk of loss, such as if a smart card is lost or stolen or a personal computer hard drive crashes. Further, security, portability and interoperability issues arise when the residence is the personal computer. Networked computers may be hacked into, thus exposing their valuable information. Also, many home computers are not mobile, thus restricting the

owner's ability to use the electronic wallet. Finally, local residence in programs such as browsers generally restrict compatibility with other applications in an effort to restrict the owner from conveniently utilizing competing browsers. Thus, local residence has some disadvantages.

A remote electronic wallet typically resides on a server. This option advantageously provides superior information protection, as the server cannot be lost or stolen. Yet, residence on a server inconveniently requires the owner to establish some sort of network connection to access the wallet. Further, remotely accessing the information brings about a problem in authenticating the identity of the individual requesting access. Passwords and Personal Identification Numbers (PINs) may be utilized, however, to increase the protection of the information. Thus, remote residence has some disadvantages.

Therefore, there exists a need to overcome some or all of the above-stated disadvantages of current electronic wallets and provide new apparatus, methods and systems for information banking.

**Summary of the Invention**

The present invention provides apparatus, methods and systems for information and financial banking. Apparatus of the present invention include virtual wallets which allow for information and financial banking. Methods and systems of the present invention include information and financial banking methods utilizing virtual wallets.

As used herein, financial banking refers to the banking, investment and securities services traditionally offered by the financial services industry. Information banking or Information-based banking is an extension of the financial metaphor where precious information is stored in a secure place on behalf of the customer. In the present invention, information is treated in a similar manner as currency. Although, "information and value" are better analogs as are "data and currency" to each other, respectively. Examples of vaulted information can include insurance policies, legal documents, medical records, in addition to financial and credit histories.

Under the present invention, a consumer's personal information can be viewed through the use of both theoretical and practical devices which characterize the

storage and value appreciation of "currency." For instance, the use of a vault to store currency can be used as a metaphor for storing and protecting information, while the investment of currency can be used as a metaphor for generating value from the transactional use of that information. Thus, the present invention provides an individual with apparatus, systems and methods to vault and invest information.

An embodiment of the present invention is a virtual wallet. Virtual wallets may be thought of as an electronic version of the physical metaphor, the conventional wallet. In one aspect, a virtual wallet of the present invention comprises software, possibly contained in special hardware, that acts as a container, for an owner/user of the virtual wallet, for at least one of the following: payment mechanisms; identity authentication mechanisms; personal information; and electronic artifacts. A virtual wallet of the present invention may also be thought of as comprising an electronic system for the secure storage, retrieval and management of personal information.

As noted above, a virtual wallet of the present invention acts as a container for electronic objects, including but not limited to payment mechanisms, identity authentication mechanisms, personal information, electronic artifacts, and the like of the owner/user of the wallet. These electronic objects are preferably not limited to information from a single source, for example a financial services institution. Instead, a virtual wallet of the present invention may be utilized to hold information from a variety of sources, including multiple financial institutions, and personal information from a variety of sources in order to provide a user with more useful virtual wallet. Many users of conventional wallets use their wallet to contain multiple bank cards, credit cards, personal information, notes, membership cards and the like from a variety of sources. In this regard, a virtual wallet of the present invention is preferably similar to a conventional wallet in terms of the types and kind of information contained in each wallet. similar to a conventional wallet.

According to the present invention, a virtual wallet may comprise one or more of the following features. A virtual wallet of the present invention may allow an owner to personalize its contents, enabling it to store any information the owner likes in a format selected by the owner. Also, an owner of the virtual wallet is able to access its contents where ever the owner may be, which along with the personalized format, maximizes the wallet's convenience. Further, a virtual wallet of the present

invention may allow an owner to link information stored in the wallet to other functions, which leverages the utility of the stored information and makes the virtual wallet interoperable with other applications. Additionally, a virtual wallet of the present invention may allow an owner to control access to and distribution of the information in the wallet, thereby giving the owner security and total control over his/her personal information. The virtual wallet systems of the present invention may advantageously feature the offering of rewards to a virtual wallet owner for distributing their information. A further feature of a virtual wallet of the present invention is that the wallet may comprise a mechanism or mechanisms that eliminate the risk of loss of the information in the wallet by remotely storing and/or disabling the wallet contents. In this way, a virtual wallet of the present invention may advantageously comprise a trusted place to keep information and valuable financial items, as well as a convenient way to move around information.

Payment mechanisms stored in the virtual wallet may comprise bank account information, credit account information, electronic currency, electronic checks and debit cards, for example. Identity authentication mechanisms stored in the virtual wallet include personal identification information and authentication information. Personal identification information may comprise, for example, name, home address, work address, home phone, work phone, emergency contact information, and biometric information. Authentication information may comprise objects such as certificates, access keys and biometric information. Personal information and artifacts of the owner that are stored in the virtual wallet may comprise, for example, the personal identification information as stated above, other personal phone numbers and addresses, appointments and reminders, personal preferences and interests, loyalty credits, coupons, pictures, tokens and tickets. The above objects are just examples of some of the exhaustive capabilities of the virtual wallet. After reading this specification other examples will be obvious to those skilled in the art.

An advantage of a virtual wallet of the present invention is that the virtual wallet may include information from a variety of sources. Further the information from different sources may interact. For example, in a virtual wallet of the present invention which includes a frequent flyer type credit card the wallet owner would be able to manage and track both credit card information and the added value function of

managing and tracking frequent flyer miles. In addition, an eclectic wallet, such as a virtual wallet of the present invention, may allow consumers to add items that are not affiliated with the wallet issuer. Allowing any item to be added to the wallet is advantageous to the consumer and other application vendors.

Another advantage of a virtual wallet of the present invention is that the virtual wallet may advantageously be a trusted place to keep information and valuable financial items. Currently there are many founded and unfounded consumer fears regarding privacy and the safety of electronic transactions. If given a choice, it seems logical that consumers would rather store their sensitive information with someone that already has a reputation for trust and consumer advocacy than a suspicious third party. In a world where information is increasingly gathered on consumers in secret, marketed, and sold, an explicit policy of privacy protection and safety is a powerful inducement to hold a virtual wallet from a financial institution. Further, there is not only value in having consumer information, but value in moving it around as well. Also like money, information can be invested to provide - increasing returns. Information must also be protected, which give rise to the concepts of information vaults and safety deposit boxes. The central issue of privacy is turned into an opportunity, and is at the core of information banking.

A further advantage of a virtual wallet of the present invention is that the virtual wallet provides a convenient way to move information around. As explained in more detail in our copending application entitled "DISTRIBUTED NETWORK BASED ELECTRONIC WALLET" (Methods and Systems for Information Banking), filed the same day as the present application and assigned serial number, _____, the disclosure of which being hereby incorporated herein by reference, a simple service of enormous convenience is to help consumers fill out forms from their personal data that resides in the information bank via their wallet. Whether a loan application, a site registration, a job application, once the information is known, there is no reason that a consumer would have to type it in again, even though it might be for different reasons, or in a different order. A further feature is that the owner of a virtual wallet may be able to have multiple answers for the same question, depending on the persona that they wish to represent at the time (social vs. work, for example).

A further advantage of a virtual wallet of the present invention is that the virtual wallet provides for selective loss, theft, and disaster recoverability. Many of the current wallet designs have deficiencies when the wallet is lost, stolen, or destroyed by disaster. It would be advantageous for a consumer to know that given one of these unfortunate mishaps, their life is not ruined. In an embodiment of a system of the present invention a new virtual wallet may be issued with no loss or corruption of data. Should the wallet be stolen, the thief will have little opportunity to make use of the information, and the wallet keys can be disabled remotely without affecting the consumers account status or the items in the wallet.

Another further advantage of a virtual wallet of the present invention is that the virtual wallet may allow for nomadic access. Current wallet designs confine one not only to the machine upon which they received their wallet items (notably certificates), but to the particular browser that obtained them. This makes it very inconvenient to a consumer if they acquire a SET certificate at home and then wish to use it at work. The present invention provides a solution is nomadic and allows the wallet to be used wherever the consumer happens to be.

A further advantage of a virtual wallet of the present invention is that the virtual wallet may be a shopping aid. One result of having consumer information is the ability to infer what they are interested in. The virtual wallet system of the present invention may allow the wallet issuer the opportunity to become a trusted electronic broker that will help consumers find what they want to buy. A further consequence is the ability to also become the consumer's electronic valet and filter out unwanted spam by knowing what they are not interested in. By recognizing that payment is only a part of commerce, and addressing other parts of commerce a virtual wallet of the present invention provides additional advantages to both a consumer and a wallet issuer.

A still further advantage of a virtual wallet of the present invention is that the virtual wallet may be an information organizer. In this regard, the virtual wallet of the present invention provides a convenient and useful way to manage and organize personal information. Further, the personal information systems of the virtual wallet of the present invention may advantageously form part of the protected information bank.

Another still further advantage of a virtual wallet of the present invention is that the virtual wallet may generate financial and non-financial rewards. In an embodiment of the present invention, part of a wallet package could be a rewards feature based upon several possible strategies. The first strategy makes discounts and special offers available to holders of the wallets. This is a familiar technique to financial service providers and is not a radical departure from what is already done today with cards and membership programs. Typically, however, the discounts and offers are of a broadcast nature and may not necessarily match a given consumers real interests. Hence, some cost of delivering the discount and offer information is wasted on consumers that are not interested.

A bolder strategy, made possible by the virtual wallet systems of the present invention, encourages consumers to make their demographics and interests available by pairing their information account (the stuff in their wallet) with a financial account. Initially, consumers are instructed to specify those things they are interested in, and an electronic shopping agent will report back to them on what it finds. The consumer interests are then categorized into profiles, less their identities, and put into a database. Instead of selling profiled mailing lists, which is perceived in a negative light by consumers, marketers would pay to have an electronic advertisement delivered to virtual wallet users of a given profile.

The information bank behind the wallet preserves the consumer's identity, while making valuable information available to marketers. These types of marketing responses are perceived as less of an intrusion to privacy since the consumer has indicated their interest by submitting a search for an item.

The value proposition of the wallet is that a portion of the money received from the marketers for delivery is passed on to the consumer into their associated financial account. In effect, the marketers are paying a consumer for their time to consider an offer. Because the marketing messages are screened through the consumer's individual profiles, the consumer will not be receiving anything that is grossly dissonant from their stated interests. Marketers will be able to get an aggregate count of how many individuals match the requested profile and a price quotation prior to an investment in delivering the ad. This allows them to refine their profile definition and tailor their marketing messages prior to large outlays of cash.

This is clearly a win-win scenario for both the consumers and the marketers. The wallet interface metaphor can be used to help the consumer track their returned value, and to enable them to move their information in and out of the "vault" area to the "information investment' area where the information is made available to profile searches.

A variant of this concept recompenses the consumers with non-monetary rewards such as loyalty credits. Loyalty credits can legitimately have a higher perceived value than a cash equivalent. Currently, loyalty programs of high demand (e.g. frequent flyer miles) are typically limited to large companies, and the rewards are not very liquid. In addition to receiving loyalty credits in return for viewing marketing messages, a virtual wallet provider could also offer a brokerage and exchange service to "swap" various loyalty credits for others. This is consistent with increasing the velocity of exchange philosophy and has an overall beneficial impact on the aggregate of loyalty programs. Suppliers benefit because they can relieve their debt faster. The "loyalty" objective is still met since consumers will join loyalty programs for products they intend to buy frequently anyway. The overall value becomes higher to a consumer because their flexibility of what they can exchange the credits for has increased, and the potential loss of earned credits due to expiration dates is reduced. Another clear win-win for consumers and marketers via the same mechanism.

Further details relating to the present invention are set forth in the appended figures and the following description.

**Brief Description of the Drawings**

Figure 1 is a schematic representation of an embodiment of a virtual wallet system of the present invention.

Figure 2 is another schematic representation of an embodiment of a virtual wallet system of the present invention.

Figure 3 is a schematic representation of an embodiment of an electronic wallet architecture according to the present invention.

Figure 4 is another schematic representation of an embodiment of an electronic wallet architecture according to the present invention.

Figure 5 is a flowchart of an intermediated transaction function of the present invention.

Figure 6 is a flowchart of a wallet open for payment function of the present invention.

Figure 7 is a flowchart of a publish public key function of the present invention.

Figure 8 is a flowchart of a purchase with coupons function of the present invention.

Figure 9 is a flowchart of a ticket purchase and use function of the present invention.

Figure 10 is a schematic diagram of the contents of an example virtual wallet of the present invention.

Figure 11 is a diagram of an example virtual wallet system of the present invention.

Figure 12 is a schematic representation of JAVA API's which may be utilized in the example virtual wallet system of the present invention.

**Detailed Description of the Invention**

The present invention provides apparatus, systems and methods that allow an individual to manage their financial and personal information. An embodiment of the present invention is referred to herein as a virtual wallet. The present invention includes virtual wallets, virtual wallet systems and methods utilizing virtual wallets.

Embodiments and features of the present invention are described in detail with reference to the appended Figures.

Figure 1 depicts a possible embodiment of the present invention. Referring to Figure 1 according to the present invention a virtual wallet may comprise a hybrid between a wallet that resides locally with the owner, 2 and a wallet that resides remotely, such as with a server, 4. A virtual wallet system further includes an interface, 6 between the local function, 2 and the server, 4. The virtual wallet system may interact with the outside world, 8 through local wallet 2 and/or the server 4. The hybrid virtual wallet combines the portability, owner control and minimized issuer resource aspects of a local wallet with the security and storage capability of a remote

wallet. Thus, the hybrid virtual wallet advantageously optimizes the advantages of each type of residence. In the following discussion, the local residence or portion of the wallet may be referred to by these names or as a "client". The remote portion of the wallet may be referred to by this name or as a "server".

The local residence of the wallet may comprise, for example, the owner's personal computer, smart card, or other similar device that enables the wallet to be utilized off-line. Typically, the local aspect of the virtual wallet, the local contents, 3 comprises data and information determined by the wallet owner to be important, while the entire wallet is contained remotely. For example, the local aspect of the virtual wallet may comprise stored value purses, important personal and authentication information, and account information enabling the local aspect of the virtual wallet to emulate any of the functionality contained within the entire wallet. The owner advantageously is able to define and have access to the most important aspects of the wallet in a convenient package that can be remotely utilized. Preferably, the local aspect of the wallet is mirrored on the remote wallet or server, thus protecting the information in case the card has to be replaced. Additionally, the local aspect of the wallet comprises a certificate or other similar authentication instrument that allows the owner to remotely gain access to the entire virtual wallet on the server. Thus, the owner can still have access to all of the wallet functionality at sites where the local aspect of the wallet can be linked to the server.

The remote aspect of the virtual wallet advantageously provides security for all of the information in the wallet. The server also provides greater storage capacity for information compared to a smart card or personal computer, for example. The contents 5, of the remote aspect of the virtual wallet comprises the entire wallet, which may be in part mirrored in a local aspect of the virtual wallet. The remote aspect of the virtual wallet, however, may not completely mirror cash and cash-like objects in the local aspect of the wallet due to off-line transactions. The present invention, however, updates the remote aspect of the virtual wallet with the latest information from the local aspect of the virtual wallet when the local wallet is on-line. Additionally, according to an advantageous feature of the present invention, the remote aspect of the virtual wallet provides privacy protection in transactions by replacing the owner's identity and address, for example, with secret information

known only to the wallet server. This feature may be utilized, for example, when marketers pay for information regarding various owner habits, preferences, etc., to give away the information without compromising the identity of the owner. Thus, the remote aspect of the virtual wallet provides security and storage capability.

Thus, this embodiment of a virtual wallet of the present invention synergistically combines the most beneficial aspects of local and remote residence into a single virtual wallet. The local aspect of the wallet is used for convenience and off-line transactions, while the remote aspect of the wallet provides for loss and theft protection.

Figure 2 also provides a schematic depiction of a hybrid virtual wallet embodiment of the present invention and a method for using same. As shown in Figure 2, a virtual wallet system may comprise a personal storage device 12, an institutional server 14 and an interface device 16. The personal storage device 12 and institutional server may each interact with the outside world, 18.

The personal storage device may comprise a smart card, personal digital assistant (PDA) or a memory chip device. The personal storage device may also comprise a computer's hard drive or other computer based storage. The preferred embodiment of a personal storage device, whether handheld and easily transportable, or a portion of a computer's hard drive, will depend on the preferences of the user of the wallet.

The personal storage device may include, but is not limited to, one or more of the following types of data: private keys; public keys; account numbers; electronic currency (e-currency); coupons; tokens; tickets; loyalty credits and the like. The functions of the personal storage device may include one or more of the following: authenticating; digital signing; or paying. These data types and functions are described in more detail in the following sections. When the wallet is on a smart card, the consumer becomes truly "nomadic" -- plug in their card wherever they go and have their wallet (and bookmarks!) available all the time. However, there will need to be capabilities built into the clients (and possibly servers) that permit this roaming feature. As the card becomes increasingly important to the consumer, means to replace lost or stolen cards must be developed just like replacement processes for

credit cards, licenses, and other physical ID cards. This will be part of the service offered by the truly useful, trusted wallet provider

The interface device need not include data but will generally include at least one of the following functions: user interface interacting; communicating; or public encryption. As will be understood from the foregoing discussion, where the personal storage device comprises a computer's hard disk and the interface device comprises the same computer, the interface device may include the data and functions of the personal storage device.

The institutional server may include the same data as the personal storage device and may further include one or more of the following types of data: certificates; names; addresses; history logs and the like. The institutional server preferably acts as backup means for the personal storage device and therefore may include back-up copies of the data contained on the personal storage device. The institutional server may include one or more of the following functions: authenticating; digital signing; paying; logging; reporting and communicating. These functions and the foregoing data types are described in more detail in the following sections.

As shown in Figure 2 by the large arrow, personal storage device 12, interface device 16 and institutional server 14 may communicate via secure interface interactions 13. In this regard, the interface device provides an interface between the personal storage device 12 and the institutional server 14. Personal storage device 12 may communicate with outside world 18 for purpose of point of sale transactions 15. These transactions include transactions involving the transfer of currency (e.g. a purchase) and also include transactions involving the transfer of personal information. The institutional server portion of the virtual wallet 14 may communicate with outside world 18 via intermediated internet transactions 17. These transactions may be handled in a manner similar to current internet based transactions and involve both the transfer of financial information (financial banking) or personal information (information banking).

From a technology point of view, virtual wallets include software programs that will reside on a smartcard, client PC/PDA/STB and/or on a server. These programs implement at least four components:

User Interface (UI). Interaction between the wallet and its the consumer will be controlled by a user interface component.

Behavior. Behaviors will be things like "pay", "add payment type", "edit personal information," etc. These will be behaviors that are available to wallet owners through the UI. It will represent the capabilities of the wallet.

Protocols. Protocols include SET, Visa Cash, Mondex, OPS (see below). These will be definitions of how the wallet needs to interact with other systems and servers. Various system implementers will provide modules that implement these protocols.

Content. Contents are consumer's specific payment accounts (credit cards, debit cards, cash) and information. This data will be unique to each consumer.

Figure 3 depicts a possible architecture for a virtual wallet system of the present invention 271. As previously noted, the concept of an electronic wallet means many things to many people. One version could be a pocket sized computer with a snap shot-size color screen that will be used in place of many essentials that consumers carry around with them today such as money, keys, identification, credit cards, tickets, as well as items that provide the consumer with mobile information and communications such as a watch, newspapers, calculator, portable telephone, pager, etc. In this embodiment, the wallet 271 is a physical thing that is carried in the pocket. Because of its electronic nature, it can add functionality that the conventional wallet can not perform. However, consumer concerns about this type of device make it impractical. Although it is technically possible to back up the contents of the electronic device, the reality is that consumers would probably be at least as irresponsible with such a device as they are currently with their own data. Further, to the extent that such a wallet interfaces with providers of the wallet or others, there is a security concern in that information about the consumer could be used by others to make a profit and not let the consumer know about it. Thus, extension of the physical wallet, especially those offered by third party software or hardware vendors make rapid adoption unlikely.

At the other end of the spectrum is the totally virtual wallet. It is not a physical device, but a set of applications on a server somewhere. The major disadvantage of this approach is that all transactions have to be "on-line" or connected

to a server. This could result in more expensive and/or less convenient use. Another issue is security.

A hybrid approach, and that preferred in accordance with the system of the invention, is to put some data and applications on a physical device and some on a server. A smart card is ideally suited for this type of application since it makes the most sense to put the security and access functions on the card, and to put the volume of data and applications on the server. Further, those transactions that would be too expensive to have on-line, such as small amounts of electronic cash transactions, also makes sense to have on a such a smart-card. Thus, as shown in Figure 3, the electronic wallet 271 in one embodiment is made up of an e-cash applications container 273, an electronic cash application manager 275, a use or authentication module 277, a key to application manager 281, a key ring applications container 283, and external applications interoperability API (applications program interface) 279, and a user application organizer and manager 285.

The e-cash applications container 273, as the name implies, is storage for e-cash applications. In order to gain critical mass, more than one type of e-cash is supported. The storage in container 273 is sufficiently generic to only record each of its members as being some form of e-cash and the actual "object" in the container 273 is a "connector" to the real e-cash application. The programming provides that the e-cash application can be located and started. The e-cash manager 275 is software that provides how to add e-cash applications and use them in a generic manner. The user authentication module 277 can be replaceable to allow for growth in the security and authentication technologies. Prior to implementation of smart cards, it could be software that asks for an account number and personal identification number, but with current technology, it can be implemented using the card and a server, using authentication technology implemented today. For future purposes, alternative security and authentication technologies might use biometrics, etc.

The key to application manager 281 serves to manage non-cash applications in the wallet such as credit, debit, e-checks, identification, facilities access and other applications. This is the software that maintains the contents of the key ring application container 283. The key-ring container 283 holds the connectors to server applications.. The contents are managed and maintained by the key to application

manager 281 previously described. Even as smart cards become more commonly available, it is believed that they will not be sufficiently large to actually hold the applications. Instead, they will hold "connectors" to the applications that reside on a server. The most important aspect of a "connector" is a key or certificate that helps identify an authorized user of the application. The "key ring" then is a container of keys. They are not like the "real" keys, however, as further illustrated by Figure 4 hereof.

More specifically, Figure 4 illustrates a wallet and application access scheme 301. In this figure, the concept of an access device provider, wallet issuer and application provider have all been separated. As illustrated in Figure 4, a consumer can use an access device 303 to access their information 305. The access device 303 has been provided at point of sale, or point of contact by some party. The wallet then uses the access device 303 and the access device server 307 connection to the network to contact the wallet issuer server 309. The consumer then identifies the appropriate application by their own description. The description is associated to an application key proxy 311 that is sent to the application provider server 313.

In the scheme 301 described, the consumer can access their information via a device 303 provided at point of sale, or point of contact by some party. Since this party will want some presence other than the device 303, some "real estate" is set aside in the presentation interface for their content. The wallet 271 uses the device 303 and the devices server 307 connection to the network 301 to contact the wallet issuer server 309. The consumer, as noted previously, identifies the appropriate application by their own description. The description is associated to an application key proxy 311 that is sent to an issuer server 309. The issuer server 309 authenticates the user and then looks up the location of the application and its real and actual key to be used for access to it. It then connects the consumer to the application at the application server 313 and serves as a secure conduit.

As may be appreciated, proxies are used instead of actual keys in case the card is lost or stolen. In this manner, the coordination with many unaffiliated organizations to issue new keys is eliminated . The issuer simply issues a new card with new proxies on the card.

A number of different features of the present invention, as disclosed in the appended Figures, will now be discussed. In all of the flow charts, each component of the system is identified along the top horizontal axis, and the description of each step is identified along the left vertical axis. Further, the middle of the chart comprises arrows, and sometimes wording, representing interaction among the system components and the flow of information. A double-headed arrow represents a two way flow of dialogue, typically with more detailed dialogue (not shown) occurring at a lower level.

The steps set forth in the flowcharts are performed by a user of the virtual wallet or implemented in computer software residing on the personal storage device, the interface or the institutional server.

**Intermediated Transaction**

Referring to Fig. 5, one feature of the present invention utilizes a wallet server to supervise a transaction between the virtual wallet and a merchant. For example, the wallet owner may be shopping at a merchant location. The wallet owner decides to purchase an item utilizing the virtual wallet. Utilizing the virtual wallet, the owner sends a purchase request to the merchant. A merchant device, such as a merchant server, receives the purchase request, verifies the item that the wallet owner wishes to purchase and sends a payment request to the wallet owner through the wallet server. The requests may be sent in the Multimedia Internet Mail Extensions (MIME) format, for example. The wallet server then forwards the request in the form of an invoice to the wallet interface, such as a browser or other similar application. The invoice is a package of information comprising, for example, the purchase order information, and the accepted payment mechanisms. Additionally, if this is an internet transaction, the invoice may also contain the URL to the acquirer server, for example. Upon receiving the invoice, the wallet owner views the invoice, selects the method of payment, and signs the invoice receipt. The signed receipt and the selected payment mechanism go back to the wallet server, which intermediates the payment transaction. For example, the wallet server may utilize the Secure Electronic Transaction (SET) protocol, or any other similar transaction protocol, to exchange the payment information such as the wallet owner's account number, the amount of the payment, and the authorizations.

Then, the final authorization or rejection is passed through to the wallet owner. Finally, the fulfillment mechanism (not shown) starts and must be received by the wallet owner to complete the transaction.

**Wallet Open for Payment**

Figure 6 represents the feature where the wallet is opened for payment and a payment request is received by the wallet server. The payment request may be in any format, such as the SET initiation MIME, JCM (JAVA Commerce Message), and Open Trading Protocol (OTP) for example. When the wallet opens, the wallet owner or user must authenticate themself to the wallet so that the wallet knows the correct user is using the wallet interface. The user may authenticate themself utilizing biometric information, PIN and password, or other similar methods. Once the wallet authenticates the user, then the wallet and wallet server must mutually authenticate each other. When the various authentication's are complete, the invoice and payment mechanisms deriving from the payment request are presented to the wallet owner through the wallet server. The wallet owner views the information through the display of the wallet interface and sends the selected payment vehicle back through the wallet server.

Next, the wallet server advantageously provides the wallet owner with a special payment authorization object for signature by the wallet owner. Traditionally, digital signatures are automatically attached to documents once a payment has been approved. In this optional feature of the present invention, however, the wallet owner goes through a step to consciously sign the invoice or receipt. Methods may be provided to capture authorization such as a digital signature.

Finally, the signed document is handled by the wallet server. The wallet server initiates and intermediates the payment transaction utilizing the appropriate protocol, such as SET or other similar protocols.

As discussed above, the method of formatting and transmitting the digital document may vary. For example, one preferred format is the extendible Markup Language (XML). This is a meta language used to describe the formats of other languages. It is a way to organize the format of data in a structured way that can be passed from computer to computer. Similarly, the format may be in Java in the form

of an object, or the format may be any other relatively standard way of encapsulating state and behavior.

**Publish Public Key**

Referring to Figure 7, another advantageous feature of the present invention is the ability to generate, publish and index a public/private key pair. An advantage of a virtual wallet system of the present invention is that the local aspect may generate a public/private key pair. The public key may be published to the server of the wallet, while the private key remains local. This feature helps preserve non-repudiation as the private key is solely in possession of the consumer. In a preferred embodiment, wherein the local residence (client) is a smart card, the private key never leaves the smart card.

This publish public key feature allows a party relying on a signed document to go straight to the issuer of a key to check it's validity, as opposed to having to check a third party's certificate revocation list (CRL). In this case, the wallet owner asks the wallet to generate a new key pair. Alternatively, this may also be a piece of software that is requested. But, in either case there may be multiple active key pairs. The chip device, after it's done the processing, returns the public key and requests from the wallet server an index to associate with it. The wallet server forwards that public key and the index request to the public key directory. This assumes that there may be two different entities -- the wallet server and the public key directory, but they may be under the same legal entity. The public key directory publishes the key and, according to a unique feature of the present invention, returns the index to this key to the wallet server. The wallet server, in turn, returns a copy to the chip device. The chip device then acknowledges the publishing of the key and the receipt of the index to the wallet owner.

Since the index may be some incomprehensible set of numbers, the present invention advantageously allows the wallet owner to associate a "friendly name" or nickname with the index. Since the wallet owner may have multiple signing keys, for different personas or different relationships, it is important for the owner to be able to create a memorable name for each key index. Finally, the chip device securely stores the index with the key pair for future use.

**Sign Digital Document**

In operation a signature requester, such as a restaurant, wants the wallet owner to sign a document, such as a receipt. The requester initiates the dialogue and sends a document to the wallet. The wallet designates the document as a signature document for recognition by the software. The wallet server sends the signature document to the wallet interface when it comes on line, thereby supporting both synchronous and asynchronous dialogs. The wallet interface displays the signature document and abstract to the wallet owner for signing. The owner then picks one of their signature key nicknames, or in other words the persona that they are signing with, and they sign the document. This feature of the present invention advantageously manages multiple signature keys.

**Purchase With Coupons**

This feature of the present invention, referring to Figure 8, advantageously provides a coupon manager system that collects coupons for the wallet owner and compares and selects appropriate coupons when the wallet owner is presented with a payment request invoice. This system beneficially allows the owner, at one time, to select and collectively redeem all coupons that apply to a particular transaction.

In this case, the wallet owner shops at a merchant and after indicating items to purchase, the merchant server sends a payment request and a list of accepted payment vehicles to the wallet owner. The payment request also comprises an invoice, and an invoice object knows the items and product numbers contained in the invoice. The invoice object delivers that list to the coupon manager, which analyzes the invoice and compares it to a coupon list that contains the coupons held by the wallet owner. After finding matches, the coupon manager prepares a list of applicable coupons and presents this list to the wallet owner. The list is preferably presented all at once, but each applicable coupon may alternatively be presented one at a time. The owner indicates which coupons to use, and the coupon manager sends the list of indicated coupons back to the merchant server as a discount request. Based on the coupons received, the merchant updates the invoice and the merchant server sends an update payment request back to the owner. The wallet owner selects a payment mechanism

and signs the payment request, which is forwarded to the merchant. Finally, the merchant authorizes the payment via conventional means, and notifies the owner of the result of the authorization.

Additionally, the coupon manager may suggest alternative purchases to the owner based on having coupons for items that are substitutes or equivalents to the items listed on the invoice. Further, the merchant may provide a coupon presentment option to the owner by offering coupons for equivalent or substitute items, or even the initially indicated items. In either case, the coupon manager presents these options to the owner for approval.

**Ticket Purchase and Use**

Referring to Figure 9, yet another feature of the present invention allows the wallet owner to purchase, store and use tickets, tokens or other similar transferable items of value. The space between lines in the chart represent the passage of time. In this case, for example, the owner interacts with a theater to purchase a ticket to a show. The theater server requests payment from the owner, who authorizes the payment. Once the theater verifies the payment, the theater server sends the ticket to the wallet server, which stores the ticket for later use. The ticket comprises a migratory object, which is able to be transferred from one location to another. When the owner decides that they want the ticket stored locally, the owner makes a request to the wallet server for local storage of the ticket. The ticket object is then transferred to the secure chip device, such as in a smart card. Upon arriving at the theater, the theater server requests a ticket and the owner plugs the chip device into the wallet interface to access the ticket, or alternatively, into a theater interface. The owner is given access to the theater once the ticket is then transferred to the theater server after a mutual authentication process.

Additional aspects of the present invention, its features, advantages and operation are illustrated in the following example.

Example

An example of an embodiment of a virtual wallet, and its use in commerce are described below and with reference to Figures 10 and 11.

The hybrid wallet is a combination of a smart card physically in possession of the user and a server based wallet. The wallet then has three distinct applications that allow it function both off-line and on-line for appropriate tasks.

The first area would be a stored value area or purse. This area would be able to dispense and track electronic cash off-line and would be re-loadable on-line.

The second area would essentially be equivalent to the magnetic strip on current cards, but allow the physical card to become a proxy for any of the cards contained in the wallet. This would allow purchases via the existing channels when the user is in physical stores. The account information would be mirrored on the server in case the card had to be replaced.

The third area represents the "rest" of the electronic wallet and is simply a entitlement that allows the holder to gain access to the wallet on the server. Such entitlements could be the form of crytograms, certificates, signed indica and the like. This provides the ability to have many wallet items when the actual resources of the cards are quite limited. Additionally, communication occurs between high-speed servers at higher bandwidths than would normally occur between a consumer's machine and a server, thus improving the overall performance.

Furthermore, should the card be lost, stolen, or destroyed, a new entitlement is easily reissued while the old one revoked. To illustrate, assume a worst case scenario that each wallet item requires its own certificate from each wallet item (application) vendor. If all of those entitlements were stored on a smart card, each vendor would have to be contacted to revoke and re-issue in the event of a card mishap. Storing the entitlements on the server avoids this complex problem and replaces it with the simple task of revoking and reissuing the one certificate that the wallet issuer has control over, the certificate to the network wallet. To the user of the wallet, where the contents actually reside may not be apparent. The *virtual* wallet appears to have all of its contents together.

The actual physical distribution of the contents, however, will be determined by what must be available off-line, and what can be resident on a server. The Figures

10 and 11 show some functionality on a smart card devoted to off-line (not on the Internet) transactions, and a single certificate to access the rest of the virtual wallet on the network.

Figure 10 provides a block diagram representing the contents of a virtual wallet. As shown in Figure 10 the owner of a virtual wallet may use the wallet to hold (contain) credit and debit cards, and related financial information. This financial currency includes in the present example, VISA® cash 122, VISA® certificates 124, VISA® credit card 126, MasterCard® credit card 128, Mondex credit 130, Mondex certificates 132, Diners Club credit card 134, MasterCard® SET certificate 136, VISA® SET certificate 138, Diners SET certificate 140. The financial currency may further include credits from selected vendors for example, Citi Shopping Network Credits 142 and Gasoline company credits 144. In addition, wallet 120 may include reward program information, such as frequent flyer miles, 146.

In addition to financial currency, the virtual wallet, 120 includes "information" currency relevant to the owner. Examples of information currency include a phone book 148, a calendar and appointment book 150, identity information 152, to do list 154, calling cards 156, personal information 158, personal interests 160 and a network wallet identity certificate 162.

Figure 11 depicts the physical embodiment of the virtual wallet 120 of the present example. As shown in Figure 11, the virtual wallet is a hybrid between a smart card 170 and a wallet server 172. Smart card 170 includes VISA® cash 122, VISA® SET certificate 138, VISA® certificates 124, VISA® credit card 126, Mondex credit 130, Mondex certificates 132 and network wallet identity certificate 162. The wallet server 172 includes MasterCard® credit card 128, Diners Club credit card 134, MasterCard® SET certificate 136, Diners SET certificate 140, phone book 148, a calendar and appointment book 150, identity information 152, to do list 154, calling cards 156, personal information 158, Citi Shopping Network Credits 142, gasoline company credits 144, frequent flyer miles, 146 and personal interests 160.

As depicted schematically in Figure 11, the owner of virtual wallet 120 may utilize the smart card portion, 170 to complete electronic cash transactions 180, for example to pay a taxi fare 182. Smart card 170 may also be utilized in credit card transactions, 184 and 186. Smart card 170 is also a proxy 188 to the server 172 or

network portion of the wallet through the internet, 190. A pass through interface allows the user to select an item (information or financial currency) from applications on the wallet server as if they were on the smart card. Since the applications and currency reside on the server, the number is not constrained by the size of the smart card's memory, and the card is easily replaced in the event of a mishap.

Additionally functionality is provided by the wallet server 172 portion of the virtual wallet 120. The wallet server, or the smart card through an interface to the wallet server, may communicate through the internet to merchant servers 192 for the purchase of goods or financial services, or the exchange of information.

Features of virtual wallet 120 may be implemented utilizing a Java Wallet Model and the Java Electronic Commerce Framework (JECF). The JECF is a set of Java API's for commerce. The JECF defines objects for commerce messages and operations. A representative schematic is provided in Figure 12.

As shown in Figure 12, the JECF includes an operations registry, 200; protocol registry 202; user interface (UI) registry, 204; instrument registry 206; and instrument instances; 208.. The operations registry supports operations for example adding or subtracting value from a card. The protocol registry allows the framework to include protocols, like SET, that effects operations like payment authorization for a credit card. The instrument registry supports financial instruments such as stored values cards or credit cards that use an underlying protocol for communication. An instrument may choose among the protocols that support it. The UI registry allows the framework to switch between different user interfaces to control the underlying base set of operations. There is also an encompassing security model for communication between objects.

The flow of an instruction within JECF is, by way of example, as follows. A java commerce message (JCM) enters the JECF. The JECF looks up and instantiates operations (downloading components if necessary). The JECF looks up a current user interface associated with the operation and displays the user interface. The JECF adds operation to the user interface and waits for operation completion by the user. A user performs an operation, interacting with the user interface. When the operation is complete a string response is returned which is returned to the caller of the operation.

The functionality of the JECF may be utilized in virtual wallet 120 with other software to perform the functions described in the preceding sections.

Although the invention has been described with reference to these preferred embodiments and features, other similar embodiments and features can achieve the same results. Variations and modifications of the present invention will be apparent to one skilled in the art and the present disclosure is intended to cover all such modifications and equivalents.

Claims

1. A virtual wallet system comprising a locally residing wallet portion, an external server residing wallet portion and an interface between the locally residing wallet portion and the external server residing portion.

2. The virtual wallet system of claim 1 wherein the wallet includes at least one of the following: payment mechanisms; identity authentication mechanisms; personal information; and electronic artifacts.

3. The virtual wallet system of claim 2 wherein the payment mechanisms comprise one or more of the following: bank account information; credit account information; electronic currency; electronic checks and debit cards.

4. The virtual wallet system of claim 2 wherein the identity authentication mechanisms comprise personal identification information and authentication information.

5. The virtual wallet system of claim 2 wherein personal information comprises one or more of the following: name, home address, work address, home phone, work phone, emergency contact information, personal phone numbers and addresses, appointments and reminders, personal preferences and interests, and biometric information.

6. The virtual wallet system of claim 5 wherein personal identification information comprises one or more of the following: name, home address, work address, home phone, work phone, emergency contact information, and biometric information.

7. The virtual wallet system of claim 5 wherein authentication information comprises one or more of the following: certificates, access keys and biometric information.

8. The virtual wallet system of claim 2 wherein the electronic artifacts comprise one or more of the following: loyalty credits, coupons, pictures, tokens and tickets.

9. A system for electronic commerce utilizing a virtual wallet of claim 1.

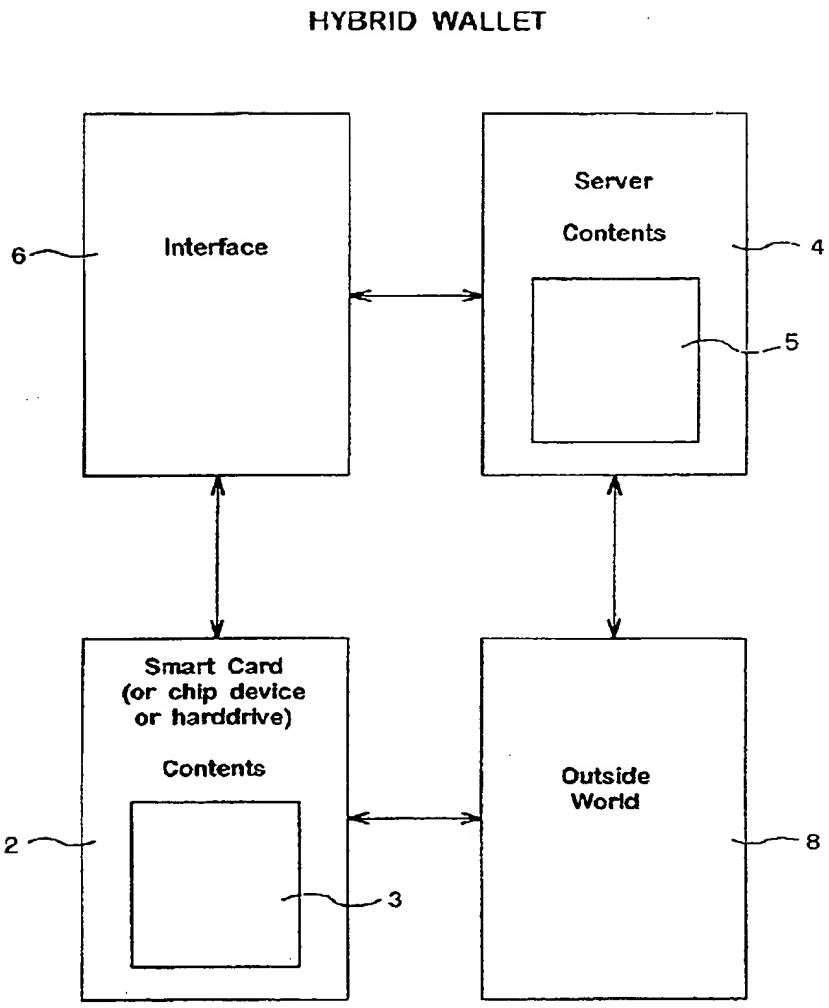
10. The virtual wallet system of claim 1 wherein the interface permits transfer of data between the locally residing wallet portion and the external server residing portion.

11. The virtual wallet system of claim 1 wherein the external server residing portion includes a mirror of information contained on the locally residing wallet portion.

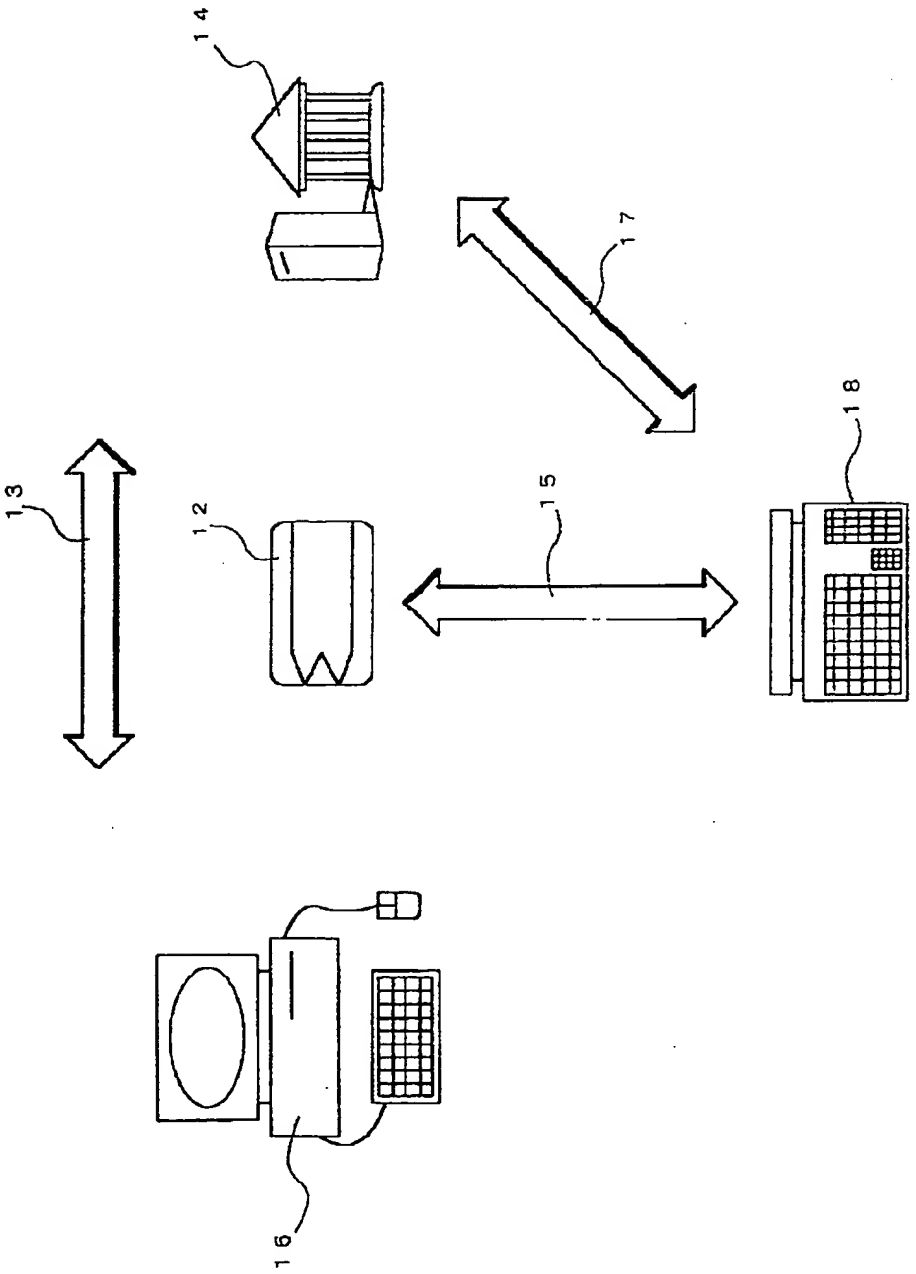
12. The virtual wallet system of claim 1 wherein the external server residing portion includes applications and the locally residing wallet portion comprises connectors to the applications that reside on the external server residing portion.

13. The virtual wallet system of claim 12 wherein the connectors comprise proxies for keys that identify an authorized user of the application.

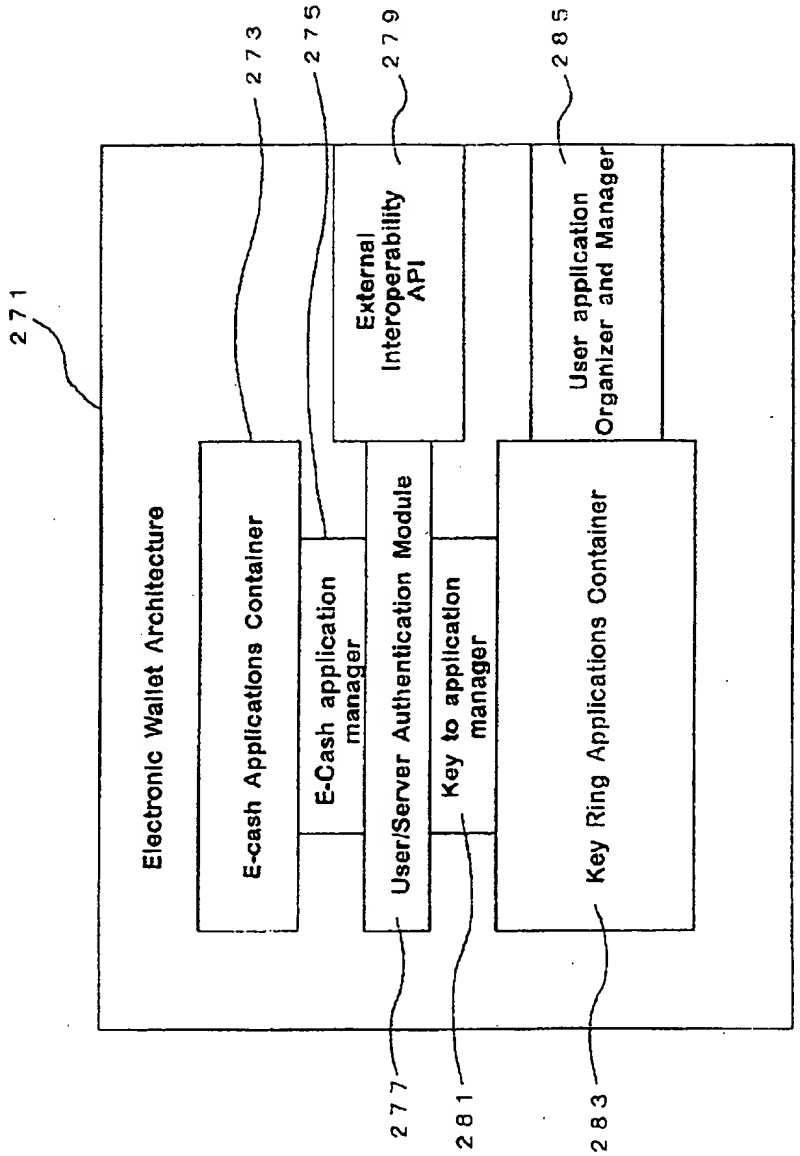
【図１】


HYBRID WALLET
Interface
6
Server
Contents
4
5
Smart Card
(or chip device
or harddrive)
Contents
2
3
Outside
World
8

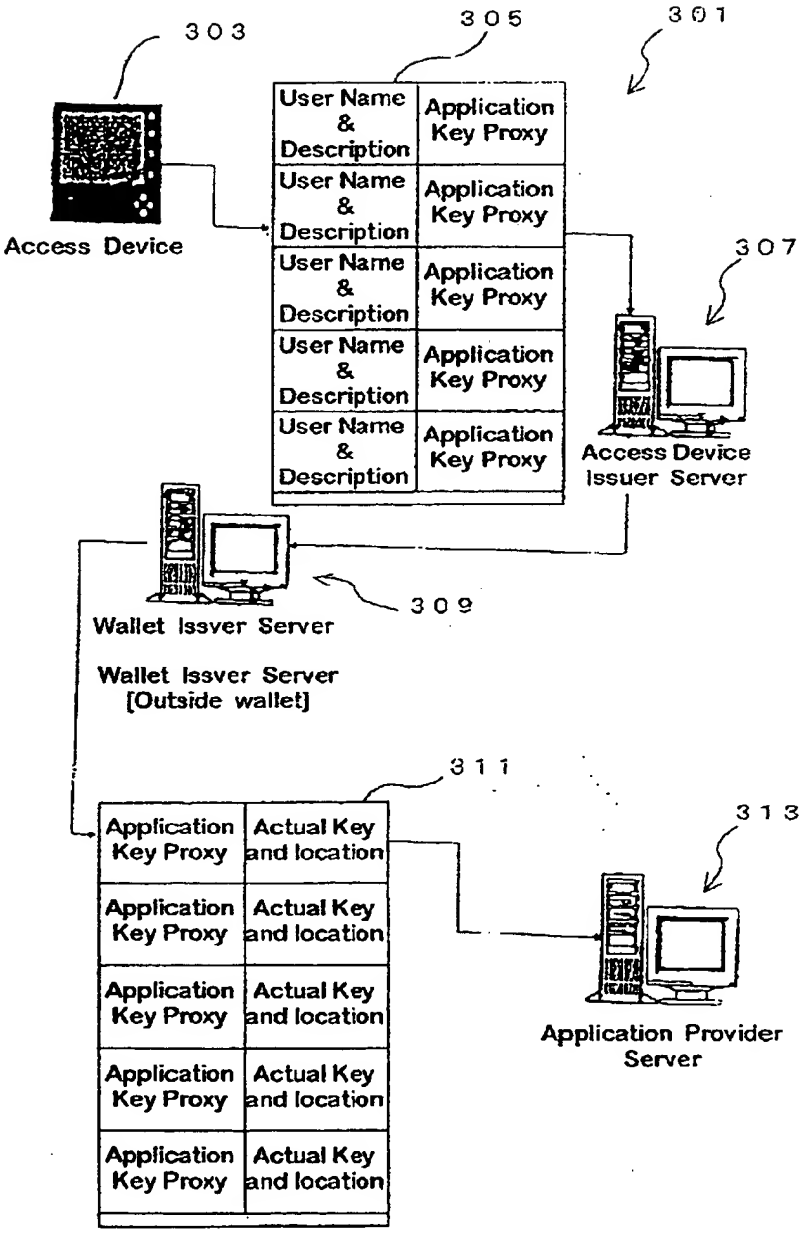
【図２】



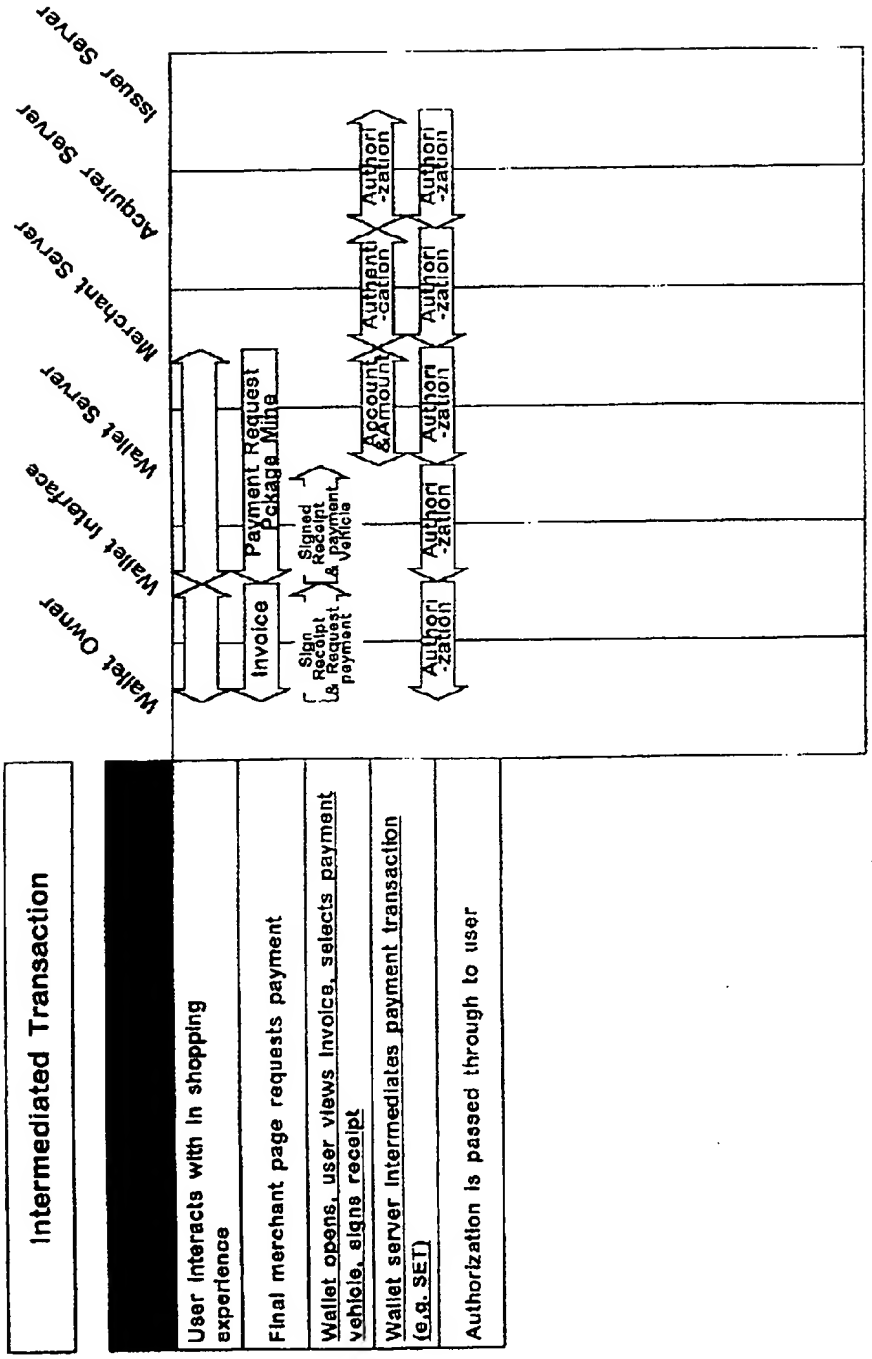
【図３】


271
273
275
279
285
Electronic Wallet Architecture
E-cash Applications Container
E-Cash application manager
External Interoperability API
User application Organizer and Manager
User/Server Authentication Module
Key to application manager
Key Ring Applications Container
277
281
283

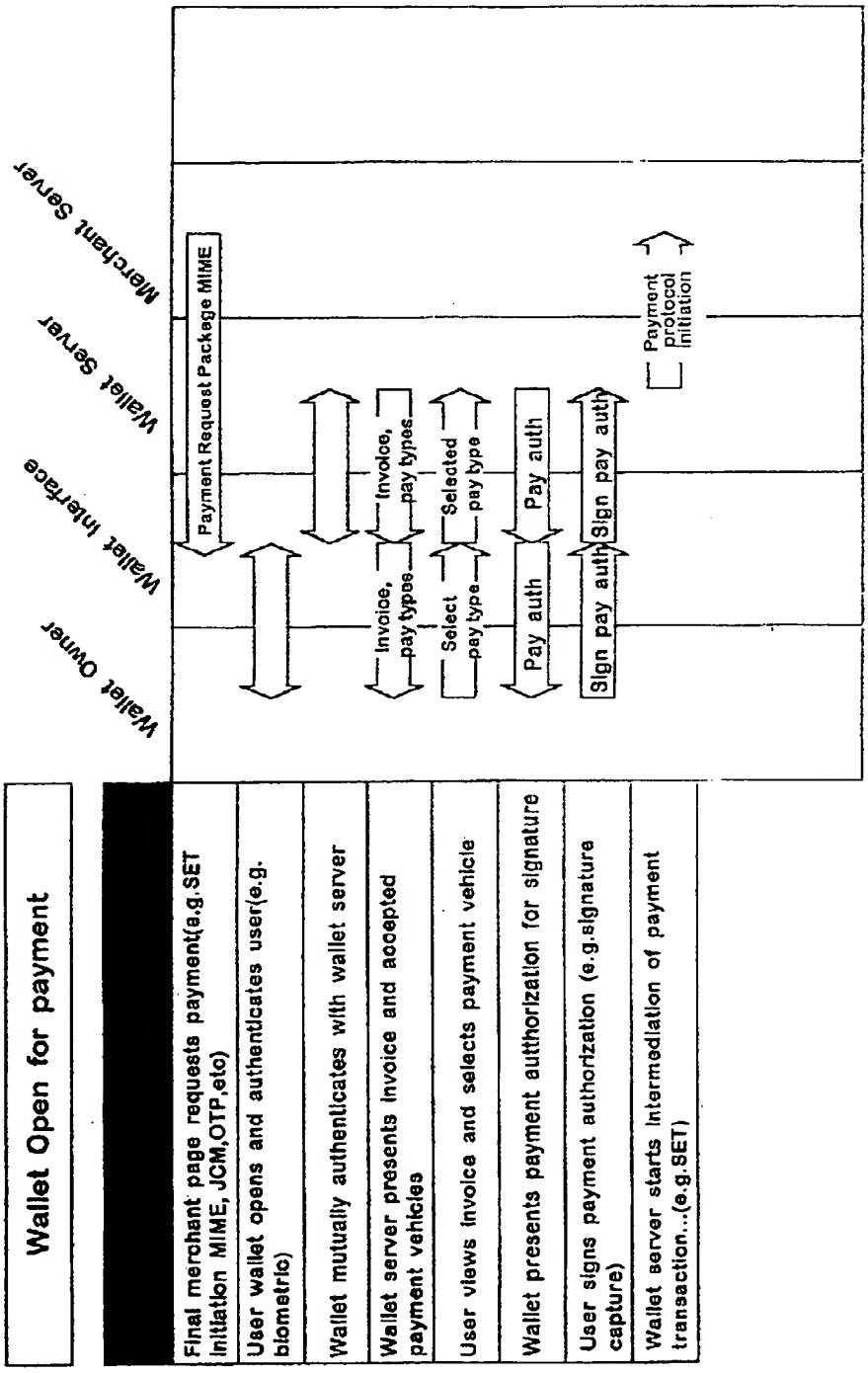
【図４】


303
305
301
User Name & Description
Application Key Proxy
Access Device
307
Access Device Issuer Server
309
Wallet Issver Server
Wallet Issver Server [Outside wallet]
311
313
Application Key Proxy
Actual Key and location
Application Provider Server

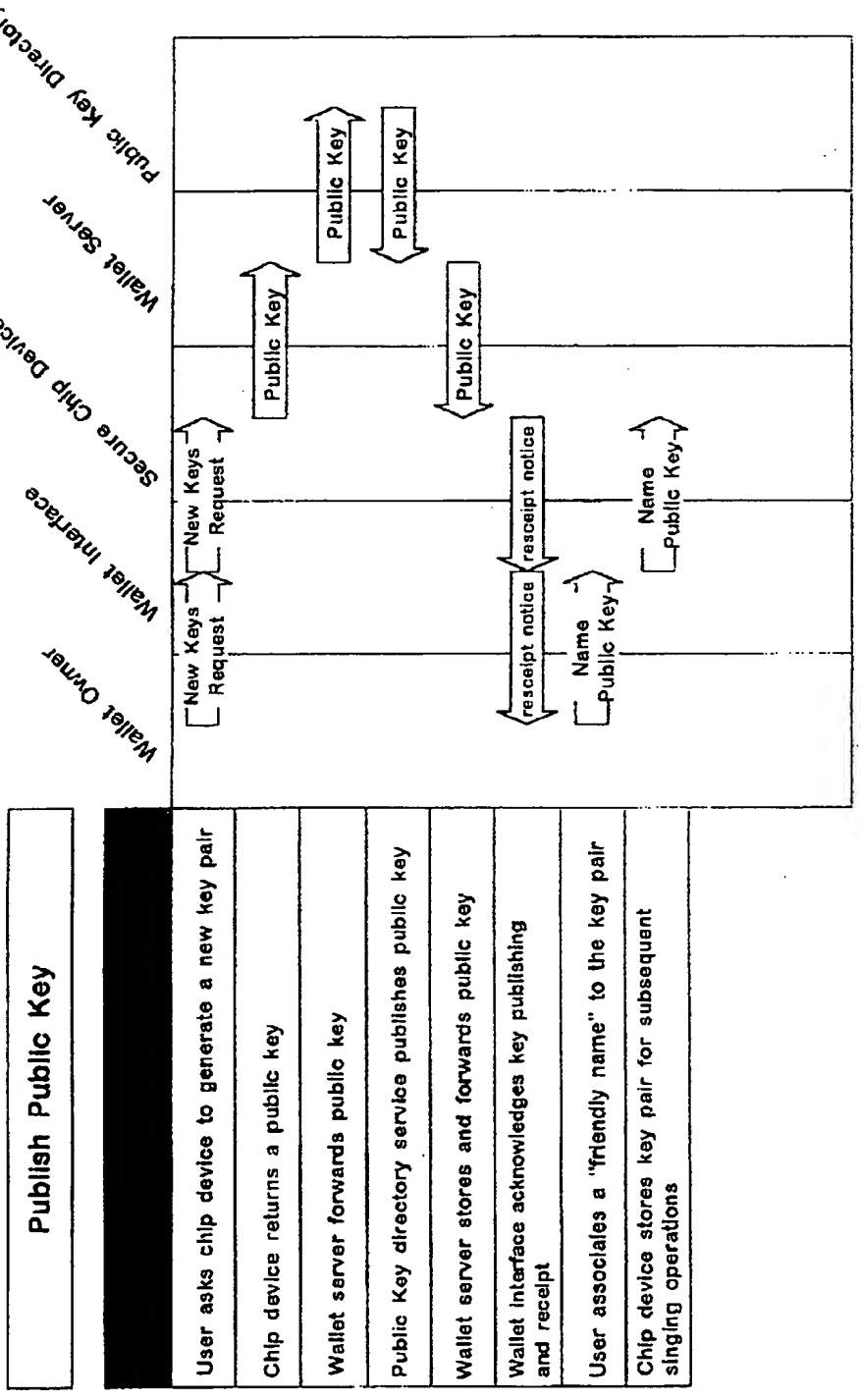
【図５】


Intermediated Transaction
User interacts with in shopping experience
Final merchant page requests payment
Wallet opens, user views Invoice, selects payment vehicle, signs receipt
Wallet server intermediates payment transaction (e.g. SET)
Authorization is passed through to user
Wallet Owner
Wallet Interface
Wallet Server
Merchant Server
Acquirer Server
Issuer Server
Invoice
Payment Request Package Mime
Sign Receipt & Request payment
Signed Receipt & payment Vehicle
Account &Amount
Authori -zation
Authenti -cation

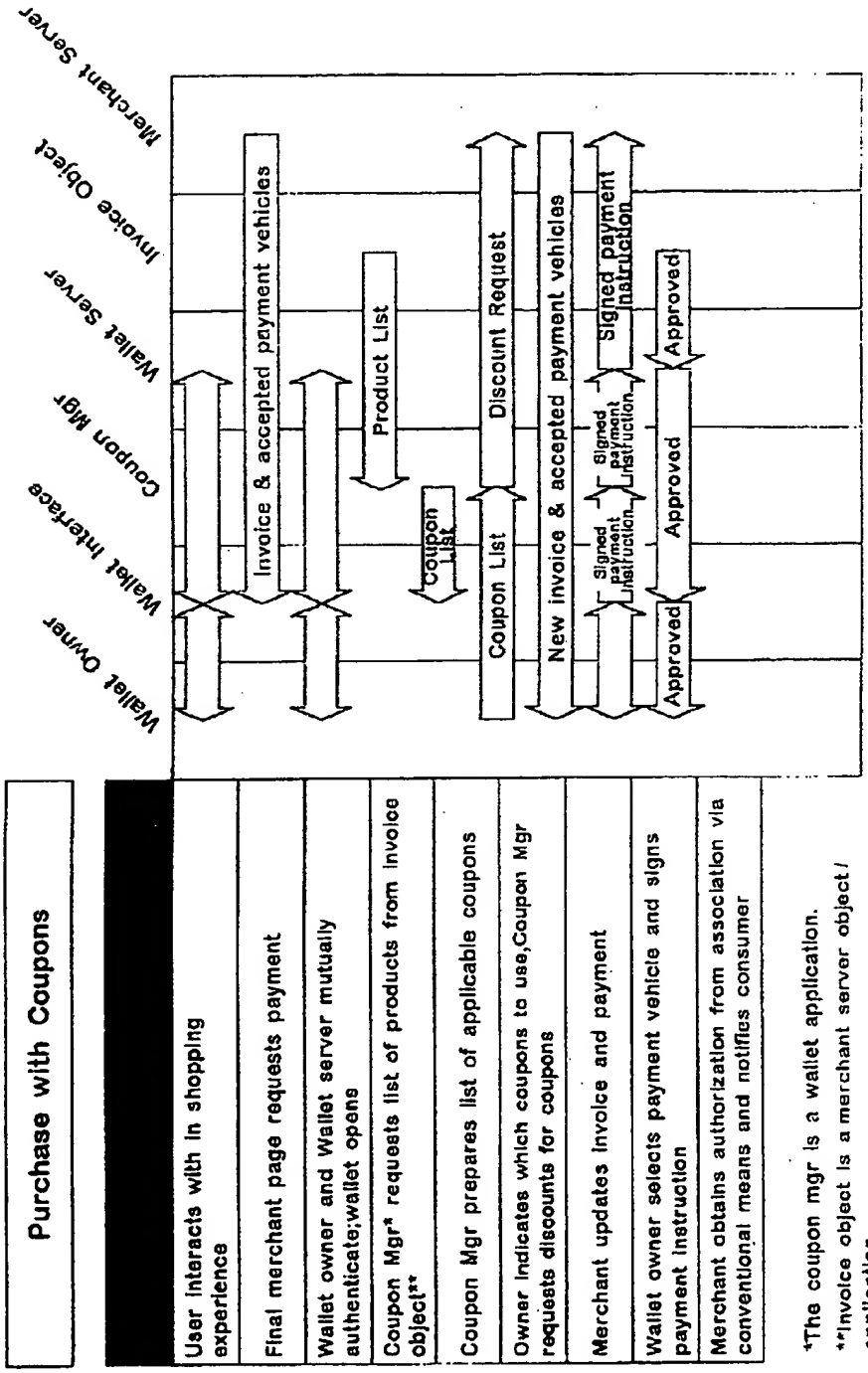
【図6】


Wallet Open for payment
Final merchant page requests payment(e.g.SET initiation MIME, JCM,OTP,etc)
User wallet opens and authenticates user(e.g. biometric)
Wallet mutually authenticates with wallet server
Wallet server presents invoice and accepted payment vehicles
User views invoice and selects payment vehicle
Wallet presents payment authorization for signature
User signs payment authorization (e.g.signature capture)
Wallet server starts intermediation of payment transaction...(e.g.SET)
Wallet Owner
Wallet Interface
Wallet Server
Merchant Server
Payment Request Package MIME
Invoice, pay types
Select pay type
Selected pay type
Pay auth
Pay auth
Sign pay auth
Sign pay auth
Payment protocol initiation

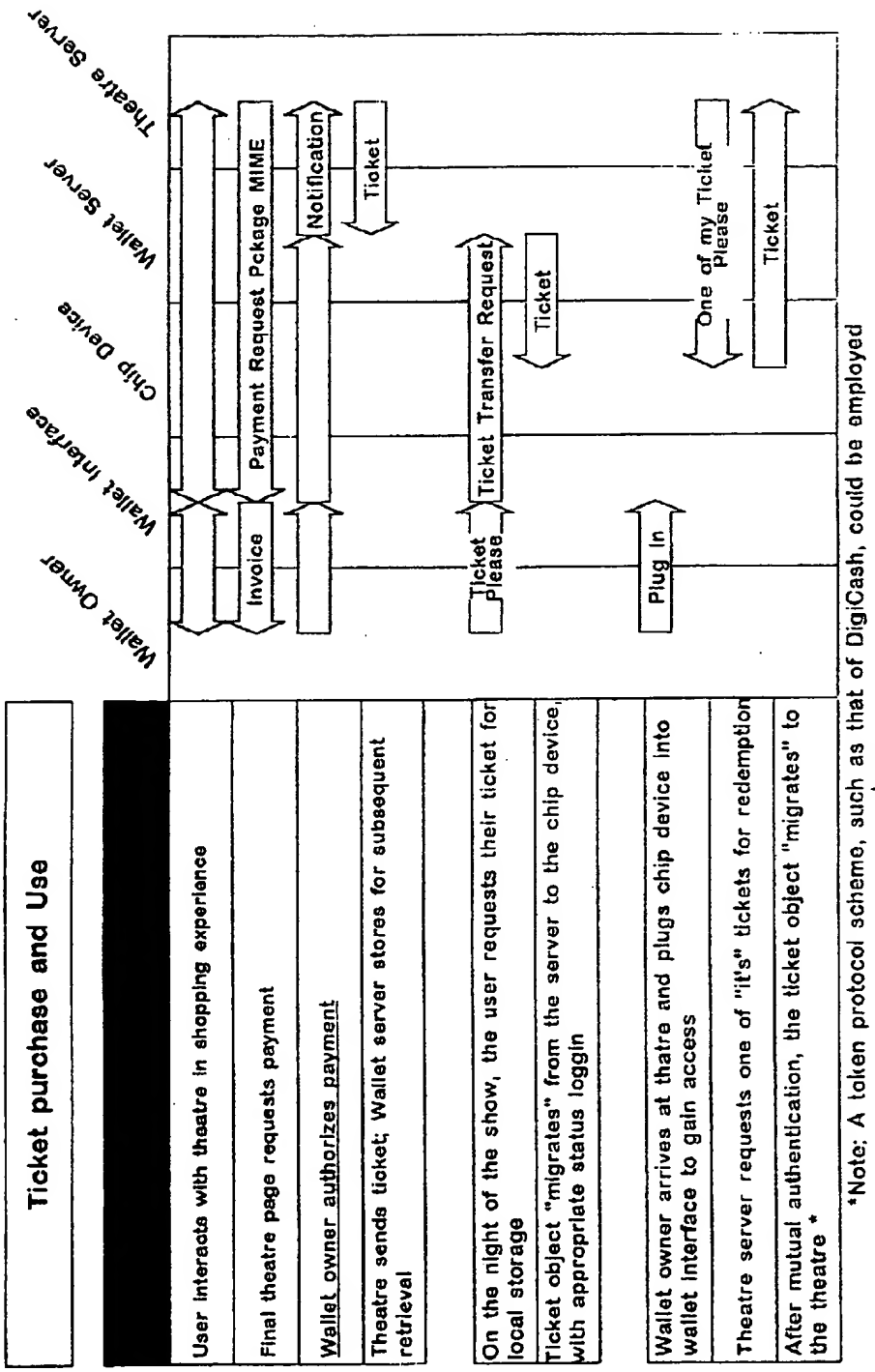
【図７】


Publish Public Key
User asks chip device to generate a new key pair
Chip device returns a public key
Wallet server forwards public key
Public Key directory service publishes public key
Wallet server stores and forwards public key
Wallet interface acknowledges key publishing and receipt
User associates a "friendly name" to the key pair
Chip device stores key pair for subsequent singing operations
Wallet Owner
Wallet Interface
Secure Chip Device
Wallet Server
Public Key Directory
New Keys Request
Public Key
Public Key
Public Key
Public Key
New Keys Request
receipt notice
receipt notice
Name Public Key
Name Public Key

【図8】

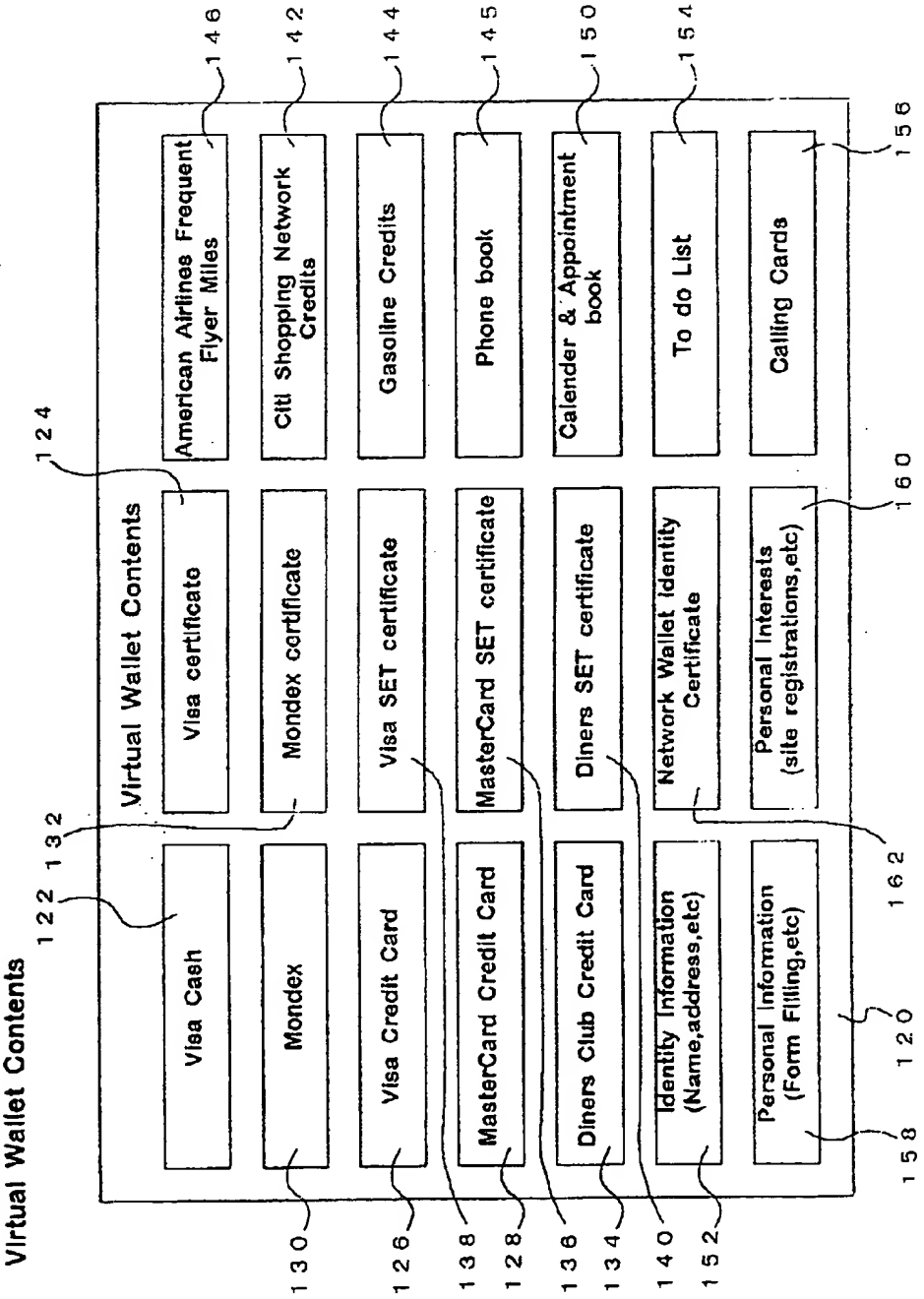

Purchase with Coupons
Wallet Owner
Wallet Interface
Coupon Mgr
Wallet Server
Invoice Object
Merchant Server
User interacts with in shopping experience
Final merchant page requests payment
Wallet owner and Wallet server mutually authenticate;wallet opens
Coupon Mgr* requests list of products from invoice object**
Coupon Mgr prepares list of applicable coupons
Owner indicates which coupons to use,Coupon Mgr requests discounts for coupons
Merchant updates invoice and payment
Wallet owner selects payment vehicle and signs payment instruction
Merchant obtains authorization from association via conventional means and notifies consumer
Invoice & accepted payment vehicles
Product List
Coupon List
Coupon List
Discount Request
New invoice & accepted payment vehicles
Signed payment instruction
Signed payment instruction
Signed payment instruction
Approved
Approved
Approved
*The coupon mgr is a wallet application.
**Invoice object is a merchant server object / application

［図９］

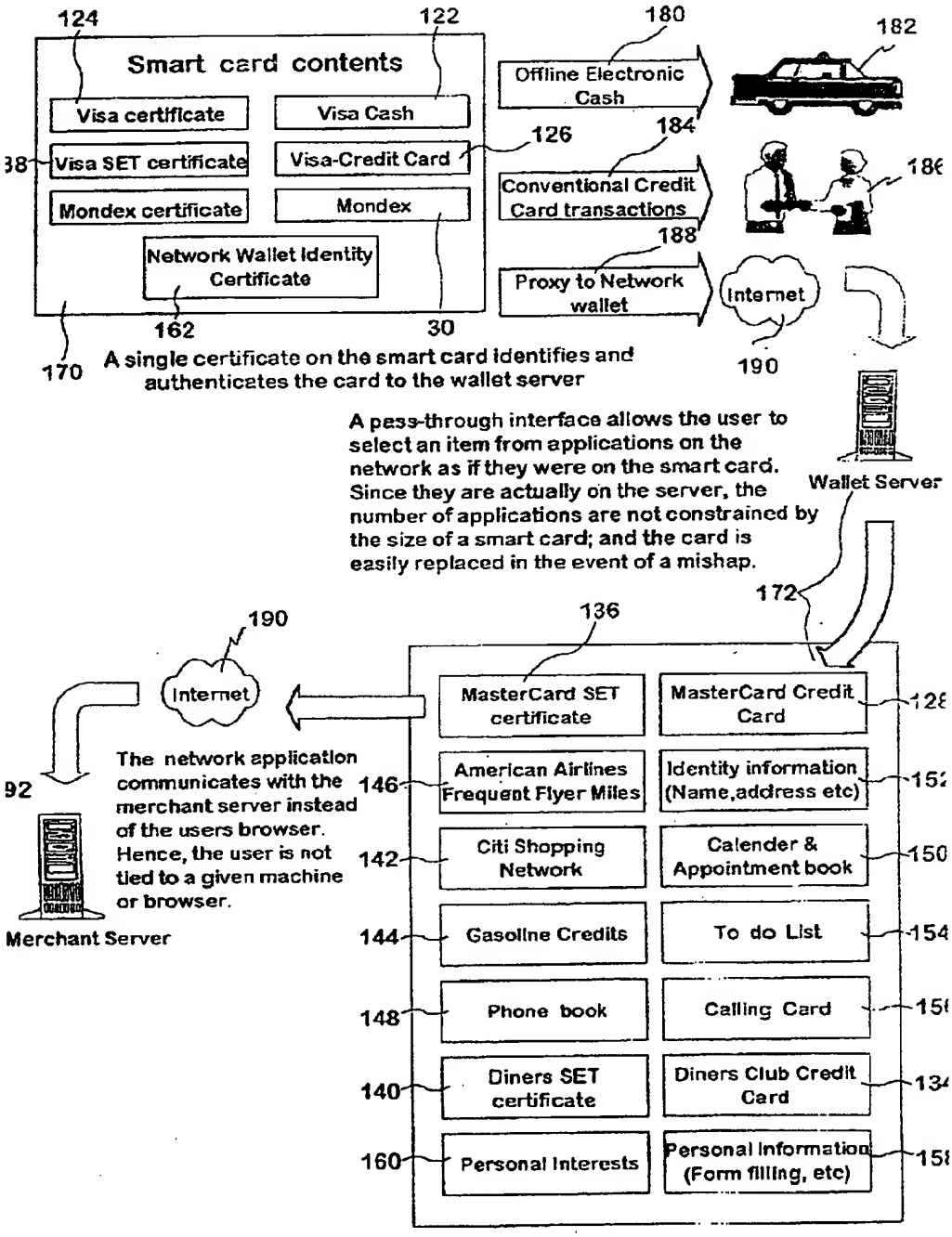



*Note; A token protocol scheme, such as that of DigiCash, could be employed here.

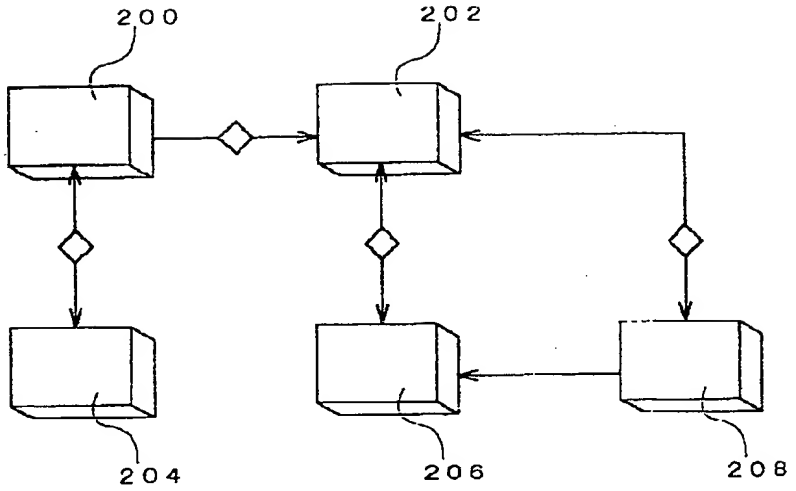
【図１０】


Virtual Wallet Contents
Virtual Wallet Contents
Visa Cash
Mondex
Visa Credit Card
MasterCard Credit Card
Diners Club Credit Card
Identity Information (Name,address,etc)
Personal Information (Form Filling,etc)
Visa certificate
Mondex certificate
Visa SET certificate
MasterCard SET certificate
Diners SET certificate
Network Wallet Identity Certificate
Personal Interests (site registrations,etc)
American Airlines Frequent Flyer Miles
Citi Shopping Network Credits
Gasoline Credits
Phone book
Calender & Appointment book
To do List
Calling Cards
122
132
124
130
126
138
128
136
134
140
152
158
120
162
160
156
154
150
145
144
142
146

【図１１】


124
122
180
182
Smart card contents
Visa certificate
Visa Cash
Offline Electronic Cash
126
184
Visa SET certificate
Visa-Credit Card
Conventional Credit Card transactions
Mondex certificate
Mondex
188
Proxy to Network wallet
Internet
Network Wallet Identity Certificate
162
30
170
190
A single certificate on the smart card identifies and authenticates the card to the wallet server
A pass-through interface allows the user to select an item from applications on the network as if they were on the smart card. Since they are actually on the server, the number of applications are not constrained by the size of a smart card; and the card is easily replaced in the event of a mishap.
Wallet Server
172
136
190
Internet
MasterCard SET certificate
MasterCard Credit Card
The network application communicates with the merchant server instead of the users browser. Hence, the user is not tied to a given machine or browser.
146
American Airlines Frequent Flyer Miles
Identity information (Name,address etc)
92
142
Citi Shopping Network
Calender & Appointment book
Merchant Server
144
Gasoline Credits
To do List
148
Phone book
Calling Card
140
Diners SET certificate
Diners Club Credit Card
160
Personal Interests
Personal Information (Form filling, etc)

【図１２】



**Abstract**

The present invention provides apparatus, methods and systems for information and financial banking. Apparatus of the present invention include virtual wallets which allow for information and financial banking including payment mechanisms; identity authentication mechanisms; personal information; and electronic artifacts. Methods and systems of the present invention include information and financial banking methods utilizing virtual wallets. A preferred virtual wallet comprises a locally residing portion and a server residing portion. An interface is provided for communication between the two portions of the wallet.

Representative Drawings; Fig.1